NIST Special Publication 500–217

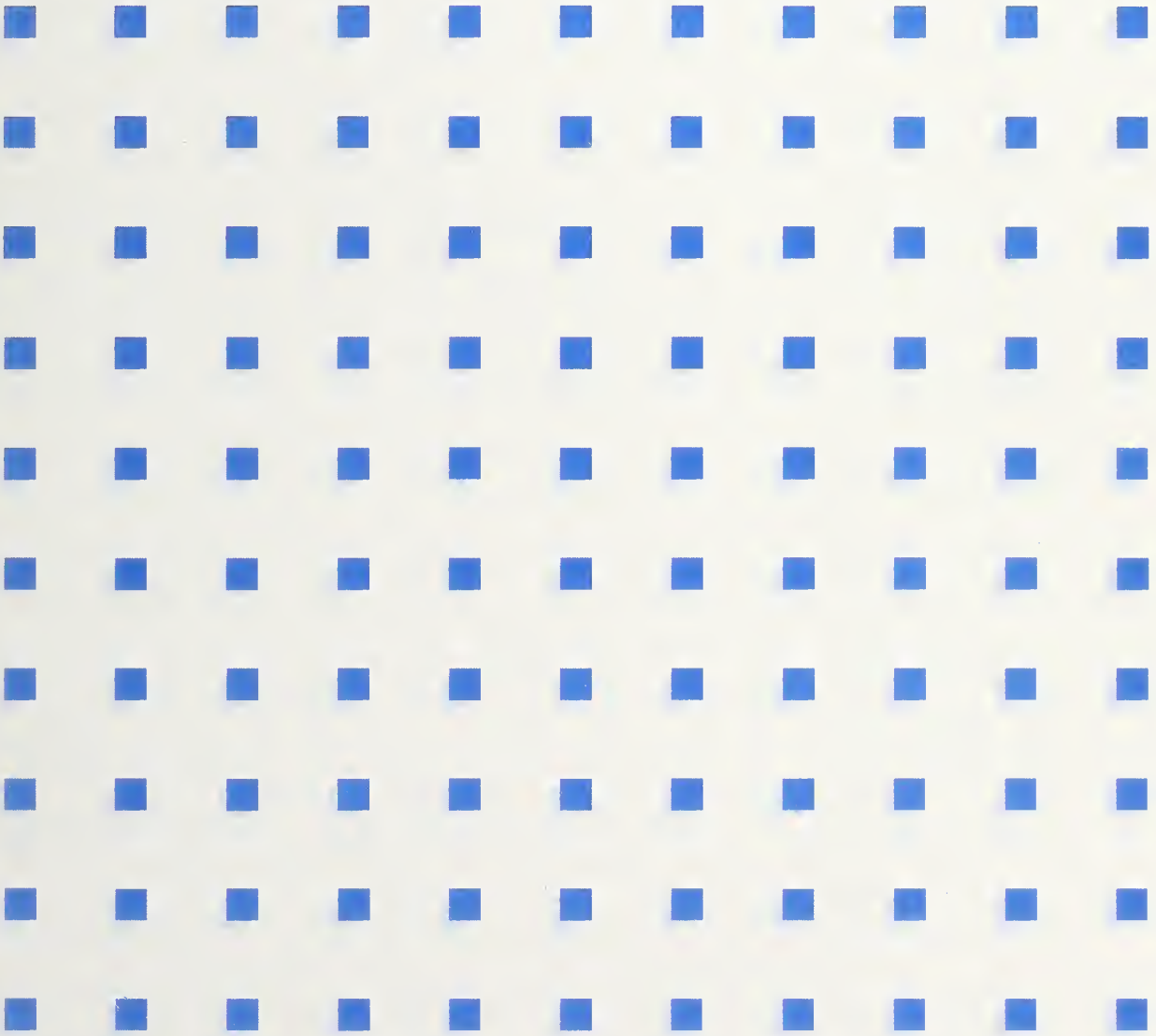
Computer Systems Technology

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

NIST

IGOSS-Industry/Government Open Systems Specification

Gerard Mulvenna, Editor



The National Institute of Standards and Technology was established in 1988 by Congress to "assist industry in the development of technology . . . needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries."

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry's competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency's basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department's Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering and performs related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST's research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Public Inquiries Desk, 301-975-3058.

Technology Services
- Manufacturing Technology Centers Program
- Standards Services
- Technology Commercialization
- Measurement Services
- Technology Evaluation and Assessment
- Information Services

Electronics and Electrical Engineering Laboratory
- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Electromagnetic Fields[1]
- Electromagnetic Technology[1]

Chemical Science and Technology Laboratory
- Biotechnology
- Chemical Engineering[1]
- Chemical Kinetics and Thermodynamics
- Inorganic Analytical Research
- Organic Analytical Research
- Process Measurements
- Surface and Microanalysis Science
- Thermophysics[2]

Physics Laboratory
- Electron and Optical Physics
- Atomic Physics
- Molecular Physics
- Radiometric Physics
- Quantum Metrology
- Ionizing Radiation
- Time and Frequency[1]
- Quantum Physics[1]

Manufacturing Engineering Laboratory
- Precision Engineering
- Automated Production Technology
- Robot Systems
- Factory Automation
- Fabrication Technology

Materials Science and Engineering Laboratory
- Intelligent Processing of Materials
- Ceramics
- Materials Reliability[1]
- Polymers
- Metallurgy
- Reactor Radiation

Building and Fire Research Laboratory
- Structures
- Building Materials
- Building Environment
- Fire Science and Engineering
- Fire Measurement and Research

Computer Systems Laboratory
- Information Systems Engineering
- Systems and Software Technology
- Computer Security
- Systems and Network Architecture
- Advanced Systems

Computing and Applied Mathematics Laboratory
- Applied and Computational Mathematics[2]
- Statistical Engineering[2]
- Scientific Computing Environments[2]
- Computer Services[2]
- Computer Systems and Communications[2]
- Information Systems

[1] At Boulder, CO 80303.
[2] Some elements at Boulder, CO 80303.

NIST Special Publication 500–217

IGOSS-Industry/Government Open Systems Specification

Gerard Mulvenna, Editor

Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-0001

May 1994

U.S. Department of Commerce
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards and Technology
Arati Prabhakar, Director

Reports on Computer Systems Technology

The National Institute of Standards and Technology (NIST) has a unique responsibility for computer systems technology within the Federal government. NIST's Computer Systems Laboratory (CSL) develops standards and guidelines, provides technical assistance, and conducts research for computers and related telecommunications systems to achieve more effective utilization of Federal information technology resources. CSL's responsibilities include development of technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive unclassified information processed in Federal computers. CSL assists agencies in developing security plans and in improving computer security awareness training. This Special Publication 500 series reports CSL research and guidelines to Federal agencies as well as to organizations in industry, government, and academia.

National Institute of Standards and Technology Special Publication 500-217
Natl. Inst. Stand. Technol. Spec. Publ. 500-217, 129 pages (May 1994)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1994

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARY

The terms defined below are used frequently throughout this profile. They are defined here to aid the non-specialist.

Protocol

In the Open Systems Interconnection reference model, the communication functions are partitioned into seven layers. Each layer, N provides a service to the layer above, N + 1, by carrying on a conversation with layer N on another processor. The rules and conventions of that N-layer conversation are called a protocol.

End System

An end system (ES) contains the application processes that are the ultimate sources and destinations of user oriented message flows. The functions of an end system can be distributed among more than one processor/computer.

Intermediate System

An intermediate system (IS) interconnects two or more subnetworks. For example, it might connect a local area network with a wide area network. It performs routing and relaying of traffic. A processor can implement the functions of both an end system and an intermediate system.

A system implementing all seven layers of protocol may provide service directly to users (acting as an end system), and it may connect subnetworks (acting as an intermediate system). When it performs the functions of an intermediate system, only the lower three layers of protocol are exercised.

Open System

An open system is a system capable of communicating with other open systems by virtue of implementing common international standard protocols. End systems and intermediate systems are open systems. However, an open system may not be accessible by all other open systems. This isolation may be provided by physical separation or by technical capabilities based upon computer and communications security.

Profile

A set of one or more base standards, and, where applicable, the identification of chosen classes, subsets, options and parameters of those base standards, necessary for accomplishing a particular function.

Subprofile

A profile subset whose boundaries have been defined on the basis of a functional separation for the purposes of convenient specification, definition of conformance, and flexibility of procurement definition. Subprofiles serve as building blocks that may be selected and combined to define a particular procurement.

IGOSS Compliance

IGOSS defines a common collection of protocol specifications (i.e., subprofiles) and minimal selection requirements that are agreed upon by the participating IGOSS organization. Each organization will develop their own profile document (e.g., US GOSIP Version 3) that specifies detailed statements of IGOSS applicability along with any additional technical requirements (e.g., additional protocol refinements and/or subprofile selection constraints). Thus IGOSS compliance is not necessarily synonymous with compliance to individual organization profiles.

None the less, few organization-specific deviations are expected. The following definitions address the notions of IGOSS compliance.

IGOSS Compliant Subprofile

An implementation of a set of one or more OSI protocols that conform to an IGOSS subprofile specification.

IGOSS Compliant System

An OSI end or intermediate system that meets the IGOSS requirements for subprofile selection.

INDUSTRY/GOVERNMENT OPEN SYSTEMS SPECIFICATION

1. INTRODUCTION

1.1 BACKGROUND

The Industry/Government Open Systems Specification (IGOSS) is jointly authored by the U.S. Government, the Canadian government, Manufacturing Automation Protocol (MAP) User Group, the Technical and Office Protocol (TOP) User Group, and the electric power industry. Each of these five major user organizations have previously issued their own procurement profiles to coordinate the acquisition and operation of computer networking products and services based on the international Open Systems Interconnection (OSI) standards.

The MAP specification [MISC 1] was first published by the General Motors Corporation in 1984. Other companies joined the effort to promote the use of the OSI protocols by the factory automation community. Under the leadership of General Motors, the MAP Users Group was formed which supported General Motors in the work of producing subsequent versions of the MAP specification. Around the same time, the office and engineering community recognized the importance of developing an OSI procurement specification which would accelerate the availablility of off-the-shelf computer networking products that would meet the needs of users. The first version of the TOP specification [MISC 2] was published in 1985 by the Boeing Corporation and, under Boeing's leadership, the TOP Users Group was formed in the latter part of that year. The MAP and TOP communities joined forces to coordinate their activities under common North American and World Federation of MAP/TOP Users Groups. The MAP and TOP specifications are now maintained by the World Federation of MAP/TOP Users Groups. The Corporation for Open Systems (COS) distributes both the MAP and TOP documents. The MAP and TOP organizations also jointly organized the Enterprise Networking Event in 1988 at which 52 vendors demonstrated that OSI products can be used to solve real business problems.

In late 1986 the National Bureau of Standards (NBS), now the National Institute of Standards and Technology (NIST), initiated development of the Government Open Systems Interconnection Profile (GOSIP). A Federal inter-agency group of experts was formed, and evolved into the GOSIP Advanced Requirements Group, that now has responsibility for promulgating each new version of the GOSIP. NIST chairs this group and has editing responsibility for the document. At the time the first draft of GOSIP was written, the MAP and TOP specifications were nearing stability, vendor OSI implementations were being successfully demonstrated, and commercial OSI products were just entering the marketplace. The intent of GOSIP is to transmit Federal user requirements to vendors and to encourage vendors to build OSI products satisfying those requirements. The GOSIP, unlike the MAP and TOP documents, is a mandate. GOSIP mandates that Federal agencies acquire OSI products when acquiring the services provided by the OSI protocols referenced in the document. Since the GOSIP must be referenced in Federal procurement requests, where applicable, GOSIP contains only those OSI protocols which are expected to be implemented in vendor products. The MAP and TOP documents included some specifications of OSI protocols which those communities wanted the vendors to implement in the future. Accordingly, although informal coordination has existed between the MAP/TOP and Federal communities, the protocols in GOSIP have tended to be a subset of the protocols in the union of the MAP and TOP documents.

In order to promote interoperability among computer systems supplied to the electric power industry, the Electric Power Research Institute (EPRI) initiated the Utility Communications Architecture (UCA) project. The first phase of the project identified the information requirements within an electric utility. Subsequent phases identified appropriate standards for inclusion in Version 1 of the UCA specification. The UCA document, like the MAP and TOP documents, is a specification of user requirements. Twenty utility companies participated in the review of the draft document, which was then formally released to the vendor

community. EPRI continues to have the responsibility for maintaining the UCA specification. OSI protocols are the foundation on which Version 1 of the UCA specification is based. The UCA authors were knowledgeable of the MAP, TOP, and GOSIP documents and recognized the importance of aligning specifications so that vendors would not be forced to build a different set of products for each new user community.

In April 1987, the Canadian federal government, announced a new policy on OSI. This policy, which applies to all Canadian government departments, endorses OSI as a Information Technology (IT) strategy in preference to any manufacturer-specific or installation-specific architecture and requires that departments and agencies state a clear preference for OSI-based products and services in their procurements. In order to assist users to migrate to OSI, work began in 1987 to develop the Canadian Open Systems Application Criteria (COSAC). This work is led and coordinated by the Treasury Board Secretariat (TBS) which is responsible for Canadian government IT standards and policy. COSAC comprises endorsements of the OSI based standards, OSI functional profiles, and guidance documents, all of which are published as Treasury Board Information Technology Standards. In producing COSAC, maximum alignment with other government and international specifications has also been an objective. Thus, cooperation between the five user communities to produce the IGOSS is just a formal extension to what has existed informally for some time.

1.2 PURPOSE

This specification is the standard reference for all IGOSS organizations to use when acquiring and operating ADP systems or services and communications systems or services intended to conform to Open Systems Interconnection protocols. This specification will allow major network users in Canada and the United States to consolidate their procurement and operational requirements in a single document and is expected to be welcomed by OSI vendors because it implicitly represents significant purchasing power.

1.3 EVOLUTION OF THE IGOSS

An IGOSS Panel, which consists of members from each IGOSS organization, is responsible for creating a procurement specification that meets the common requirements of the participating user groups. Since the IGOSS will be referenced in procurement requests, the document can only include functionality which vendors are in the process of implementing or have already implemented.

For this version and all subsequent versions of the IGOSS, the IGOSS Panel, after consulting with members of their respective organizations, recommends the protocols and services to be included in the common procurement specification. In making this decision, the IGOSS Panel considers the progress made in developing the standards and implementors agreements and the commitment of the vendors to develop products based on these documents. The IGOSS Panel members are then responsible for obtaining formal concurrence on the proposed content of the draft document from the organizations that they represent. Members of IGOSS organizations, as well as industry and government reviewers, will use a 90 day public comment period as the mechanism to comment on the document. The IGOSS Panel will then modify the draft version of the IGOSS, incorporating those comments which are consistent with the objectives of the IGOSS organizations. The panel members will then obtain final approval of the document from their respective organizations before publishing the document in final form. (The IGOSS will be published as a NIST special publication in the United States and as a Treasury Board IT Standard in Canada.) This approval process will apply when each new version of the IGOSS is issued.

IGOSS will be updated by issuing new versions at appropriate intervals, tentatively every 2 years, to reflect the progress being made by vendors in providing OSI products with new services for government and commercial uses. A new version of IGOSS will supersede the previous version of the document. Every attempt will be made to obtain backward compatibility with the previous version of the document. Every

new version of IGOSS will specify the architecture and protocols that were included in each of the previous versions so that the protocols added to each version can easily be determined.

1.4 SCOPE

In an increasingly complex world, the need to exchange information has become an ever more important factor in conducting business. Until recently, computer networking technology has not kept pace with this need to communicate. Even now, many users have "islands" of computer systems built by different vendors, or even by the same vendor, that cannot exchange information. The IGOSS indicates that, in response to this, the vendor community has developed a nonproprietary solution for this requirement to exchange information. The solution uses OSI protocols, allowing computer systems built by different vendors to exchange data. These OSI protocols give users access to standardized applications which can operate over diverse reliably interconnected subnetworks. The IGOSS lists the protocol specifications and provides procurement alternatives.

IGOSS significantly expands the scope of user services provided by OSI applications. The IGOSS electronic mail service uses the OSI standard for Message Handling Systems (MHS). There are two major MHS components: the Message Transfer System (MTS) and the cooperating user agents. IGOSS specifies two types of user agents for which International Standardized Profiles are currently under develpment. Additional user agent (UA) types may be specified by procurers. The two internationally standardized User Agents are the Interpersonal Messaging User Agent, used to send a personal message from an originator to one or more recipients, and the Electronic Data Interchange User Agent, used to send and receive business related tranactions using standard transaction sets. File transfer services are provided by the File Transfer, Access, and Management (FTAM) application. A remote terminal access capability is provided by the Virtual Terminal (VT) application. The Directory Services application provides access to a distributed directory on behalf of human users or OSI applications such as MHS or FTAM. The Remote Database Access (RDA) application allows the interconnection of database applications resident in heterogeneous environments. The Transaction Processing (TP) application provides for reliable support of distributed, interdependent transactions. The X-Windows application allows a user to gain access to multiple computer applications by dividing a screen into multiple sections, each section responding independently to input from a keyboard or a pointing device or both. The Manufacturing Messaging Specification (MMS) application allows objects related to a process control environment to be accessed and manipulated across a network. The Information Retrieval (IR) application provides information search and retrieval by converting queries constructed in a local query language into a common representation. All of these applications use lower layer OSI protocols to guarantee that end systems attached to subnetwork technologies [e.g., X.25 Wide Area Network (WAN), Local Area Network (LAN), Integrated Services Digital Network (ISDN), Frame Relay] can interoperate.

1.5 RELATIONSHIP OF THE IGOSS TO EXISTING PROFILE DOCUMENTS

The IGOSS is a collaborative effort of organizations that have previously published the Canadian Open System Application Criteria, the Manufacturing Automation Protocol specification, the Technical and Office Protocol specification, the United States Government Open Systems Interconnection Profile and the Utility Communications Architecture documents. Documents will continue to be published by the responsible IGOSS organizations, but now they will primarily refer to the IGOSS to specify the OSI procurement requirements for each organization. The documents will also contain specifications for any protocol required by the organization, but not agreed to in common, and an applicability statement which indicates how the IGOSS must or should be used.

1.6 APPLICABILITY

The IGOSS specifies a set of OSI protocols for computer networking that is intended for acquisition and use by IGOSS organizations. Each IGOSS organization will specify the applicability of IGOSS to its own members. The detailed statements of applicability will appear in supplementary profile documents, issued by each IGOSS organization.

1.7 IGOSS FUNCTIONALITY

Version 2 of GOSIP was the base document used to prepare the IGOSS. All GOSIP Version 2 protocols are included in the IGOSS. The functionality added to the base document to form Version 1 of the IGOSS is as follows:

1. Message Handling Systems (CCITT 1988 Recommendation);
2. Electronic Data Interchange (EDI) User Agent;
3. File Transfer, Access, and Management (FTAM) - (Phase 3);
4. Virtual Terminal Service (S-mode Paged and X.3 profiles);
5. Directory Services;
6. Remote Database Access;
7. Transaction Processing;
8. Manufacturing Message Specification;
9. X-Windows over OSI;
10. Information Retrieval;
11. Fiber Distributed Data Interface (FDDI);
12. Frame Relay;
13. Point to Point Protocol (PPP);
14. Intermediate System-Intermediate System routing (IS-IS) protocol;
15. Inter-Domain Routing Protocol (IDRP);
16. Network Management protocols; and
17. Connectionless Upper Layer services.
18. Minimal OSI Upper Layer Services

1.8 SOURCES OF PROTOCOL SPECIFICATIONS

1.8.1 Primary Source

1.8.1.1 Relationship of the IGOSS Protocol Specifications to Workshop Agreements

The primary source of protocol specifications in the IGOSS is the Stable Implementation Agreements for Open Systems Interconnection Protocols [NIST 1], hereafter referred to as the Workshop Agreements. By primary source, it is meant that where the IGOSS uses a given protocol, it cites that protocol by reference to the Workshop Agreements. The primary source is used in all instances where the protocol of interest has been specified in the Workshop Agreements. Section 4 of this specification augments those agreements when necessary to provide the functionality required by IGOSS organizations.

The primary source document was created and is maintained by the Open Systems Environment (OSE) Implementors Workshop (OIW). The Workshop Agreements provide implementation specifications that are derived from service and protocol standards issued by the International Organization for Standardization (ISO) and the Consultative Committee for International Telegraphy and Telephony (CCITT). A copy of the Workshop Agreements is essential to thoroughly understand the material in this document.

A new version of the Workshop Agreements is created each year, following the December OSE Implementor's Workshop meeting, if a sufficient amount of new functionality has accumulated since the previous version was issued. It is the intent of the Workshop that new versions of the Workshop Agreements be backwardly compatible with previous versions. Replacement pages applying to the latest version of the Workshop Agreements may be published at regular intervals during the year. These replacement pages may contain errata to the original stable agreements that are approved by the Workshop plenary. The latest replacement pages are distributed to all workshop attendees and are available through several sources. (See NIST Reference 1 for ordering information.)

Each new version of the IGOSS will reference the latest appropriate version of the Workshop Agreements as the base document. These agreements, although stable, can be modified by errata which correct technical and editorial mistakes or by changes which are required to align with evolving international standards or agreements developed in other regional workshops. These changes to the Workshop Agreements are stabilized each December and become effective as an Implementation requirement the following December (e.g., the stabilized Workshop Agreement for December, 1993 becomes effective as an implementation requirement as of December, 1994). This becomes effective with the December, 1993 Workshop Agreements.

Each version of the IGOSS is issued in draft form for public comment before it is issued in final form. Final editions of the IGOSS will reference only the Stable Workshop Agreements. [Editors Note: The authors of the IGOSS reserve the right to reference agreements that are not yet stable (i.e., Working Agreements) in the draft edition, as long as these agreements are envisioned to be stable by the time the final edition of the IGOSS is published. The final edition of the IGOSS may reference a later version of the Stable Workshop Agreements than is referenced by the draft edition, so that agreements that became stable during the interval between the draft and final edition can be included.]

1.8.1.2 Relationship of the IGOSS Protocol Specifications to International Standardized Profiles

International Standardized Profiles (ISPs) are functional profiles which are approved for publication by the ISO/IEC JTC1 Special Group on Functional Standards (SGFS) under SGFS procedures. These functional profiles should be technically harmonized at the regional workshop level before submission to the SGFS.

It is a goal that the IGOSS technical specifications reference ISPs, when possible. The linkage by which this will occur will be the Workshop Agreements. For each protocol, the appropriate Special Interest Groups will determine if and when it is appropriate to replace the existing Workshop Agreement text with a reference to an ISP.

1.8.2 Secondary Sources

The IGOSS must be complete in that open systems procured in accordance with it must interoperate and must provide service generally useful for government and commercial computer networking applications. The Workshop Agreements continue to evolve, but remain incomplete. (The appendices of the IGOSS cite needed work.) Thus, where the Workshop Agreements are not complete, the IGOSS may augment protocol and service specifications from the following sources.

- o International Standards and Recommendations
- o Draft International Standards
- o Institute of Electrical and Electronics Engineers (IEEE) Standards
- o Working Implementation Agreements from the OIW

Since this profile is one of open systems, the secondary sources include specifications that are international standards or are advancing to become international standards. They are included in the IGOSS, where

needed, to help satisfy the criterion of utility. Note that secondary sources exclude protocols, however mature, that are not a part of the international standards process.

1.8.3 Tertiary Sources

Even the secondary sources named above may not provide a complete and useful networking system today. It may be necessary for the IGOSS to augment protocol and service specifications from the following sources.

- o National Standards
- o Government Standards
- o Military Standards
- o Other publicly available specifications

The use of specifications from other than the primary and secondary sources is undesirable. It is expressly intended that these omissions from standards work be brought to the attention of the international standards bodies so that acceptable international standards may be developed as rapidly as possible. The IGOSS Panel will replace all tertiary source protocols in the IGOSS with suitable primary and secondary sources, as soon as they are available.

1.9 IGOSS ERRATA

All errata to the IGOSS will be subject to the same public review process that exists for the IGOSS document. The errata may take effect at any time after the public review period if approved by the IGOSS Panel. Since each new version of the IGOSS will supersede the previous version, errata to previous versions will be published in subsequent versions.

2. DESCRIPTIONS OF ARCHITECTURE AND PROTOCOLS

This section briefly describes the IGOSS specification and networking architecture. For a more thorough understanding, consult the User's Guide [NIST 7] and other references cited in this profile.

2.1 SPECIFICATION ARCHITECTURE

IGOSS includes a wide variety of application services, lower layer communication services and subnetworking technologies (See Figure 2.1). It is not a requirement that any one system will support all of the capabilities defined in IGOSS. Instead, it is expected that acquisition authorities will select a subset of capabilities that meet specific communication requirements.

To facilitate this process IGOSS defines a number of *subprofiles* as building blocks that may be selected and combined to define a particular procurement. Subprofiles define the specific multi-layer protocol requirements for the provision of a chosen service or subnetwork technology.

IGOSS provides the acquisition authority with 3 major classes of subprofiles:

- *Application subprofiles* - define the upper (i.e., Application through Session) layer requirements for support of specific user services (e.g., Message Handling Systems).

- *Lower layer subprofiles* - define the Network and Transport layer requirements for support of specific end-to-end communication services in various networking environments.

- *Subnetwork subprofiles* - define the Network, Data Link, and Physical layer requirements for support of direct system attachment to specific subnetwork technologies.

This partitioning of OSI services and protocols reflects the independence of user requirements for upper layer application services, lower layer communication services, and use of specific real subnetwork technologies.

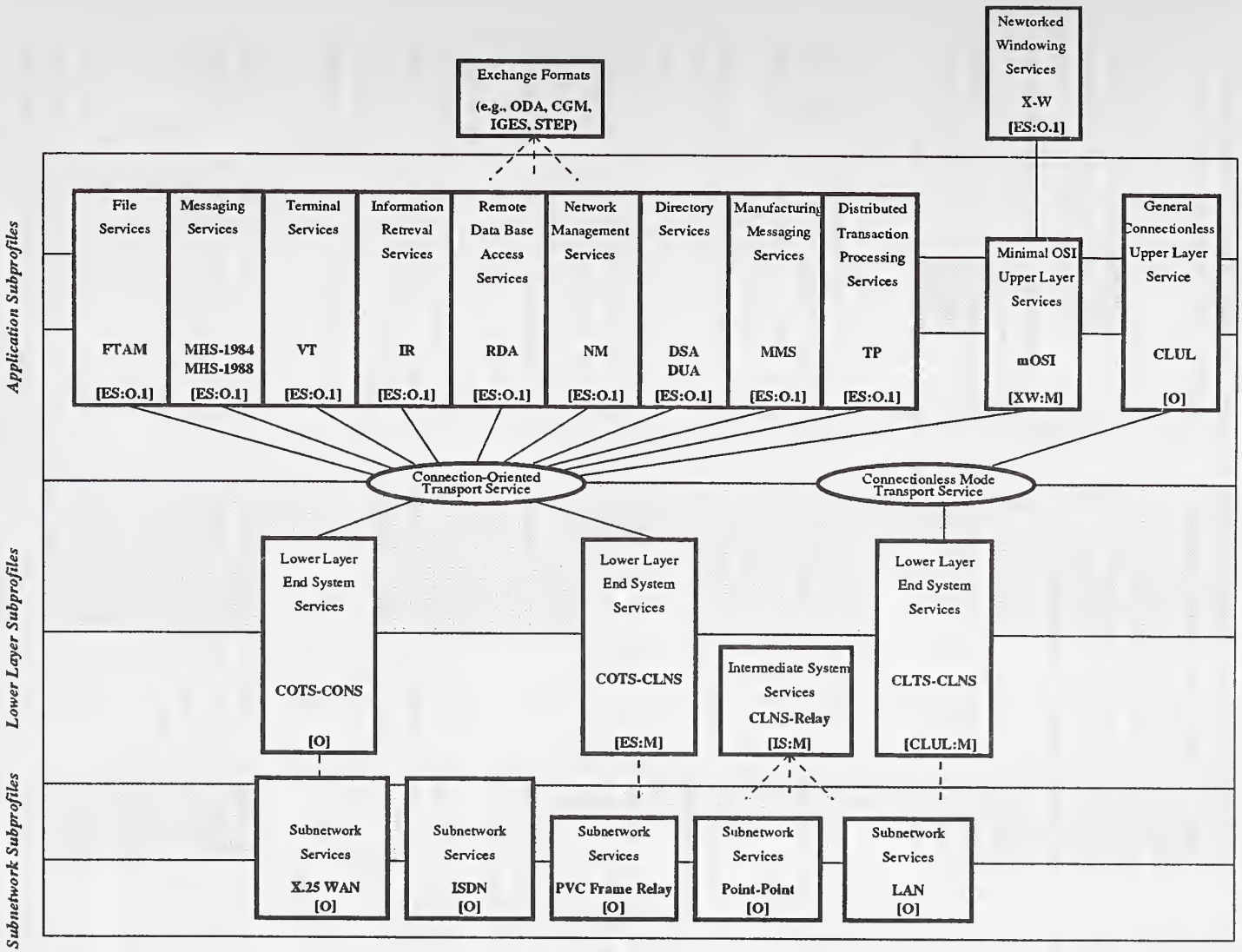
The determination of subprofile boundaries or interfaces has been made on the basis of a functional separation for the purposes of specification, definition of conformance, and flexibility of procurement. It is not required that IGOSS subprofiles, or specified combinations of subprofiles, be implemented as discrete products. Implementors are free to adopt any internal system architecture for the implementation of OSI services and protocols specified in IGOSS subprofiles.

Within a given subprofile there may be major procurement options that relate to the support of optional functionality, the role in which a system operates, or other similar issues. These options parameterize a given subprofile into specific product procurement categories that must be specified by the acquisition authority. Procurement categories in Version 1 of the IGOSS may have variables which are explained in the section in which they appear. All Procurement categories will appear in bold face typeset.

In general, the acquisition authority has the flexibility to choose the subprofile combinations to be supported within a system. Where there are technical restrictions on the correct or advisable subprofile combinations, the subprofile definitions will state appropriate binding rules and recommendations. Likewise, certain restrictions may be placed on the selection of subprofiles for the purpose of effecting policy aimed at insuring an overall viable, interoperable networking architecture. These restrictions are implemented by making the support of some subprofiles mandatory while requiring others to remain as optional additions.

Figure 2.1 depicts the components of the IGOSS specification and networking architecture. The figure shows combinations of subprofiles that can be selected to define a complete networking procurement. Each subprofile denotes its selection status using a Protocol Implementation Conformance Statement (PICS)-like notation (e.g., [0.1]).

Again, the subprofile boundaries and interfaces depicted in the figure are not meant to constrain the internal architecture or product configuration of IGOSS implementations. For example, different application protocols may use a common implementation of OSI upper layer services through the use of ACSE/Presentation service Application Programming Interfaces (APIs). See Section 3.1.2 and Appendix 5 for more details on APIs.



Subprofile Selection Key

[M]	**Mandatory**
[O]	**Optional**
[O.<n>]	**Optional, but at least one of the group of options labelled by the same numeral <n> is required.**
[<c>:<s>]	**Conditional. If <c> is TRUE then the status is <s> else the status is O.**

2.2 NETWORKING ARCHITECTURE

IGOSS provides a wide variety of standard OSI application services to support various end user data communication requirements (e.g., file transfer, messaging, virtual terminal, information retrieval, remote database access, networked windowing, directory, manufacturing messaging, transaction processing, and network management). Each application may require a different set of services from the Application, Presentation and Session Layers. Thus, most IGOSS application subprofiles specify the layers 5, 6 and 7 requirements for each application service.

OSI provides several, potentially non-interoperable, options for lower-layer data communication services. Achieving OSI in large user communities is best accomplished by using a single method (subprofile) to perform the functions of end-to-end reliable data transfer. To assure interoperable data transfer for a variety of applications across a variety of subnetwork technologies, IGOSS mandates support of lower-layer services provided by Transport Protocol Class 4 (TP4) and the Connectionless Mode Network Protocol (CLNP). The use of TP4 and CLNP provides a common basis for reliable end-to-end communication across all types of subnetworking technology. The support of appropriate subprofiles based upon TP4 and CLNP (i.e., COTS-CLNS in end systems, and CLNS-Relay in intermediate systems) is mandatory for all IGOSS systems.

IGOSS provides additional, optional, choices for the provision of lower-layer communication services. In particular, IGOSS includes subprofiles for the provision of Connection-Oriented Transport services over the Connection-Oriented Network Service (i.e., COTS(X)-CONS) and the Connectionless Mode Transport Service over the Connectionless Network Service (i.e., CLTS-CLNS) as procurement options. The specification of these subprofiles is sufficient for achieving interworking among IGOSS systems that additionally choose to support these optional lower-layer services.

It is useful to enable user selection from among a set of subnetwork technologies for local and wide area networking. These different technologies exhibit physical, performance, and cost differences that render one technology more appropriate than others for particular uses. IGOSS provides a wide variety of standard subnetwork technologies (e.g., LAN, X.25 WAN, ISDN, Frame Relay, Point-to-Point links) through the definition of Subnetwork Subprofiles. One, or more, subnetwork subprofiles must be specified for each real subnetwork interface of a system.

In circumstances in which specific deployment requirements can not be met by any of the technologies provided by the IGOSS1 subnetwork subprofiles, other technologies may be used. In such cases the acquisition authority must provide a proper subnetwork subprofile specification, including conformance requirements, so as to ensure the procurement of an effective product; that is, a product that is capable of supporting the selected IGOSS lower layer subprofiles and can interoperate with other IGOSS systems to be attached to the subnetwork.

IGOSS also addresses a number of supporting services and ancillary issues (e.g., exchange formats, naming and addressing, security, and management information) related to the provision of OSI data communications. While some of these issues are not directly concerned with the procurement of OSI protocols, they are included to allow the acquisition authority to define an effective environment for the deployment and use of IGOSS protocols.

A goal of this profile is to permit an acquisition authority to issue unambiguous procurement requests for standard applications operating over networks using standard protocols. The acquisition authority determines the required applications and the required networking environment and the IGOSS defines the appropriate subprofiles. For example, if an acquisition authority requires a general purpose File Transfer Access and Management service with management agent support, on a "thin-net" Carrier Sense Multiple

Access/Collision Detection (CSMA/CD) LAN subnetwork, IGOSS provides the following subprofile combination:

1. IGOSS1 FTAM (RR)
2. IGOSS1 Network Management
3. IGOSS1 COTS-CLNS
4. IGOSS1 LAN (CSMA/CD, 10Base 2)

The specification of this subprofile combination is sufficient to define an interoperable file transfer service in the required networking environment. Note: All subprofiles in the first version of the IGOSS begin with IGOSS1.

2.3 PROTOCOL DESCRIPTIONS

Following are brief narratives of the general services provided by protocols in each layer of the IGOSS architecture to the layer above.

The Application Layer (layer 7) allows for protocols and services required by particular user-designed application processes. Functions satisfying particular user requirements and application service elements (See sec. 3.2.1) that can be used by more than one application are contained in this layer. Representation and transfer of information necessary to communicate between applications are the responsibility of the lower layers. See Section 3.2 for the references that apply to each IGOSS application.

The Presentation Layer (layer 6) specifies or, optionally, negotiates the way information is represented for exchange by application entities. The Presentation Layer provides the representation of: 1) data transferred between application entities, 2) the data structure that the application entities use, and 3) operations on the data's structure. The Presentation Layer is concerned only with the syntax of the transferred data. The data's meaning is known only to the application entities, and not to the Presentation Layer. See References [NIST 1; ISO 1,20,21,24,25]. The Presentation Layer also supports a simple connectionless presentation service [ISO 57].

The Session Layer (layer 5) allows cooperating application entities to organize and synchronize conversation and to manage data exchange. To transfer the data, session connections use transport connections. During a session, session services are used by application entities to regulate dialogue by ensuring an orderly message exchange on the session connection. See References [NIST 1; ISO 1,14,15; CCITT 12,13]. The Session Layer also supports a simple connectionless session service [ISO 58].

The Transport Layer (layer 4) provides either connection-oriented or connectionless, transparent transfer of data between cooperating session entities. The Transport Layer entities optimize the available network services to provide the performance required by each session entity. Optimization is constrained by the overall demands of concurrent session entities and by the quality and capacity of the network services available to the Transport Layer entities. In the connection-oriented transport service, transport connections have end-to-end significance, where the ends are defined as corresponding session entities in communicating end systems. Connection-oriented transport protocols regulate flow, detect and correct errors, and multiplex data, on an end-to-end basis. See References [NIST 1; ISO 1,12,13; CCITT 10,11]. See references [ISO 46-47] for the connectionless transport service option.

The Network Layer (layer 3) provides packet routing and relaying between end systems on the same network or on interconnected networks, independent of the transport protocol used. The network layer may also provide hop-by-hop network service enhancements, flow control, and load leveling. Services provided by the network layer are independent of the distance separating interconnected networks. See References [NIST 1,3; ISO 1-8,11; CCITT 1; NCS 1].

The Data Link Layer (layer 2) provides communication between two or more adjacent systems. The data link layer performs frame formatting, error checking, addressing, and other functions necessary to ensure accurate data transmission between adjacent systems. Note that the data link layer can operate in conjunction with several different access methods in the physical layer. See References [NIST 1-3,5; ISO 1,26,28; CCITT 1].

The Physical layer (layer 1) provides a physical connection for transmission of data between data link entities. Physical layer entities perform electrical encoding and decoding of the data for transmission over a medium and regulate access to the physical network. See References [NIST 1-3; ISO 1; ISO 29-31].

3. PROTOCOL SPECIFICATIONS

3.1 SUBPROFILE SPECIFICATIONS

The individual subprofile and interface specifications in this section are designed to be used directly in Requests for Proposals. However, acquisition authorities must take additional steps to ensure a specification which fully meets their requirements. Any additional requirements should be stated as modifications or additions to the IGOSS subprofile specifications in the sections that follow.

3.1.1 Subprofile Selection

The networking architecture described in Section 3 suggests a range of choices of subprofiles that span the layers of the OSI reference model. Clearly, a subset of these subprofiles may adequately satisfy an individual acquisition requirement. The acquisition authority has the responsibility to select and combine IGOSS subprofiles to define an effective procurement that meets user data communication requirements.

The selection of IGOSS application subprofiles is based upon user requirements for data communication services and the policy requirements of this specification. There are no other restrictions on the combinations of application subprofiles that can be selected for a given system.

IGOSS also provides, as an option, a generic Connectionless Upper Layers (CLUL) subprofile. While no IGOSS1 applications use these connectionless upper layer services, the CLUL subprofile is provided to support non-IGOSS applications that may require such services.

Most IGOSS application subprofiles require the support of the Connection-Oriented Transport Service (COTS). Appropriate lower layer end system subprofiles (e.g., COTS-CLNS, and optionally COTS(X)-CONS) must be selected to provide lower layer services for these applications. The CLUL application subprofile requires the support of the Connectionless Mode Transport Service (CLTS). If the CLUL application subprofile is selected, the CLTS-CLNS lower layer end system services must also be selected.

The selection of lower layer services are dictated by the OSI communication role(s) that a system performs, the service requirements of application subprofiles, and the subnetwork technologies over which it must operate. To assure interoperability over the widest range of real communication environments, IGOSS mandates the support of subprofiles based upon Transport Class 4 (TP4) and the Connectionless Network Protocol (CLNP). Thus, for end systems, support of the COTS-CLNS subprofile is mandatory. For intermediate systems support of the CLNS-Relay subprofile is mandatory. These mandatory lower layer subprofiles can be combined with all IGOSS subnetwork technologies.

Additional, optional lower layer end system subprofiles may be selected by the acquisition authority. In particular, IGOSS provides the option of supporting the Connection Oriented Network Service (CONS) in the COTS(X)-CONS subprofile. Likewise, the CLTS-CLNS end system lower layer services may be selected to support the CLUL application subprofile.

At least one subnetwork subprofile must be specified for each real subnetwork interface of the system. Some subnetwork technologies can only be combined with a subset of the IGOSS lower layer subprofiles. The acquisition authority must examine the requirements stated in the Lower Layer and Subnetwork Subprofile definitions to determine the valid combinations.

3.1.2 Service Interface Requirements

The IGOSS mandates no service interface accessibility beyond that indicated in the Workshop Agreements; therefore, any additional service interface accessibility requirements must be clearly stated and mandated by the acquisition authority. IGOSS mandates no specific direct access to transport services although existing conformance tests require access to the Transport layer service boundary. If the acquisition authority requires direct access to transport services, such a requirement must be included in a solicitation. The issues involved in determining such a requirement are complex. Refer to the User's Guide [NIST 7] for a discussion of these issues.

Should an acquisition authority not request direct access to service interfaces, such access might or might not be provided at the discretion of individual vendors. For example, some vendors may provide access to session services, others may provide access to transport and network services, and still others may limit access to association control services only. Of course, some vendors may provide direct access to service interfaces at the human user interface only. When there is no requirement for a service interface between layers, vendors might merge multiple layer implementations. Such a merger is often implemented to accrue performance benefits to the user.

Should an acquisition authority request direct access to a specific service interface, care should be taken to specify the general functional and operational objectives of the interface; otherwise, particular vendor interface implementations might or might not meet user requirements.

While specifying the general functional and operational objectives for a service interface should enable the vendor to meet a user's functional requirements, such a specification will not ensure portability of software, written to the interface, across product lines from multiple vendors. Work is underway in the IEEE POSIX networking services interface committee to create a series of Application Program Interface (API) specifications that will enable portability of software written to those specifications. The IEEE has standardized API specifications for the Message Handling Systems [IEEE 1-2] and Directory Services [IEEE 1,3] applications. It is recommended that these APIs be specified in procurement requests when there is a requirement to develop portable software that interfaces with these applications. The IEEE is currently developing APIs to other OSI services which will be referenced in a future version of the IGOSS. See Appendix 5 for further information.

When APIs do not exist, acquisition authorities requiring service interfaces that enable software portability must include a very detailed and explicit interface specification within the solicitation. Such a specification is difficult and expensive to produce, and will limit the number of vendors that bid on a solicitation. Thus, this practice is not recommended. A more prudent course, at the present time, is to specify the general functional and operational objectives of a service interface, leaving implementation decisions to the vendor.

3.2 APPLICATION SUBPROFILES

This section contains the Application Layer subprofiles which operate in conjunction with OSI lower layer subprofiles to provide services which meet many government and commercial user requirements. Procurement categories are listed for each application. These procurement categories are intended to assist users in making high-level procurement decisions, particularly those affecting interoperability with other systems; they are not intended to provide a complete procurement specification. Users should consult the User's Guide [NIST 7] and, where applicable, the appropriate Evaluation Guidelines [NIST 9-10, 15] for additional information useful in specifying procurement requirements and evaluating vendor proposals.

3.2.1 Common Application Service Elements

Application Service Elements (ASEs) provide common Application Layer services that allow the exchange of information among application processes. The ASEs used by one or more of the IGOSS applications are described in the following subsections. The ASE(s) used by each application will be specified in the corresponding application subprofile figure.

The Association Control Service Element (ACSE) [ISO 22-25] controls the association between two Application Entities; it is responsible for establishing and releasing an association. Certain information, such as the identity of the application processes and the supporting Application Service Elements, must be agreed between the Application Entities before the association is established. The ACSE, as specified in Part 5, clause 5 of the Workshop Agreements, is required to support all IGOSS applications except the CCITT 1984 Message Handling Systems application.

3.2.1.2 Remote Operations Service Element

The Remote Operations Service Element (ROSE) provides the facilities to invoke a remote operation on another computer, to have the result of the operation or an error message returned to the invoker, or to have the remote operation rejected as invalid. ROSE [ISO 50-51] can be used by the Common Management Information Protocol and the CCITT 1988 Message Handling Systems and Directory Services applications. ROSE must be implemented as specified in Part 5, clause 6 of the Workshop Agreements.

3.2.1.3 Reliable Transfer Service Element

The Reliable Transfer Service Element (RTSE) provides the facilities to reliably transfer large amounts of data between distributed application processes. RTSE uses the Activity and Minor-synchronize functional units of the Session Layer to set checkpoints in a large data string so that data transfer can be restarted at a convenient point if the underlying network connection breaks. RTSE [ISO 52-53] is used by the CCITT 1988 Message Handling Systems application and optionally, by the Directory Service application, and must be implemented as specified in Part 5, clause 7 of the Workshop Agreements.

3.2.1.4 Commitment, Concurrency and Recovery Service Element

The Commitment, Concurrency and Recovery (CCR) Service Element provides the facilities to insure that a series of multi-party operations completely succeed or, if not, to ensure that a rollback to the initial state occurs. CCR [ISO 54-55] is used by the Transaction Processing application to implement provider supported transactions and must be implemented as specified in Part 5 of the Workshop Agreements.

3.2.1.5 Transaction Processing User Application Service Element

The Transaction processing protocol does not provide an explicit protocol for transmitting user data. The Transaction Processing (TP) Service standard provides a TP-DATA service. This service is implemented in the protocol by the User Application Service Element (U-ASE). The Transaction Processing standard specifies a general mechanism which allows a set of programs to interact in a controlled manner. Because it is a general mechanism, it was impossible to specify what data would flow between programs; this is in sharp contrast to X.400, for example, in which data flows were able to be architected by the standards committee. The U-ASE is both separate from and part of the TP program. It is a part of the TP program because it is crafted to encode and decode its data stream. A U-ASE made for a specific data stream is useful only to programs that need that data stream. It is separate from a program because it can be used by many programs. A TP program can use two different U-ASEs to communicate with different types of users. For example, an accounts payable query program might use different U-ASEs to communicate with

different classes of users. The program would generate the same data stream. The U-ASE could filter, encrypt or simply encode the data for transmission depending on where the end-user was located.

3.2.2 File Transfer, Access and Management

The File Transfer, Access, and Management (FTAM) standard [ISO 2-6] allows for the effective transfer, access, and management of different file types on remote systems by creating a virtual filestore which emulates the file services offered by existing file service systems. Transfer occurs using the virtual filestore which is then mapped onto the real filestore when the transfer is complete.

An FTAM system must support one or more of the following procurement categories.

"IGOSS1 FTAM (IS)"
"IGOSS1 FTAM (IR)"
"IGOSS1 FTAM (RS)"
"IGOSS1 FTAM (RR)"

An FTAM implementation can operate as an initiator of remote file activity, as a responder to requests for remote file activity, or as both initiator and responder. Further, FTAM implementations can operate as senders (of data to receivers), receivers (of data from senders), or both. Thus, in the procurement category listed above, X can be one or more members of the set that specifies the four possible roles: "IS" (initiator-sender), "IR" (initiator-receiver), "RS" (responder-sender) and "RR" (responder-receiver). The acquisition authority must determine the requirements for each FTAM device in terms of above-mentioned roles.

All FTAM systems must support implementation profiles T2.3 (Positional File Transfer), M1.3 (Management) and A1.3 (Simple File Access) as they are described in Part 10 of the Workshop Agreements. Each of these implementation profiles requires the support of certain document types and makes the support of other document types optional. If the procurement authority requires the support of an optional document type, it should be so stated in the procurement request.

Figure 3.2.2 shows the application subprofile for FTAM implementations. The upper layer support requirements for FTAM are specified in Part 5, clause 13.1 of the Workshop Agreements. In addition, all FTAM systems must support the Restart-Data-Transfer and Recovery functional units as specified in Part 10 of the Workshop Agreements.

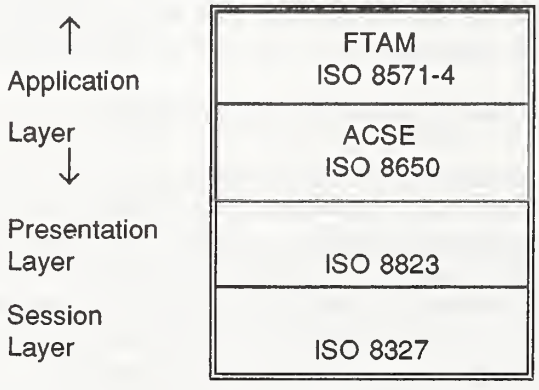


Figure 3.2.2. FTAM Application Subprofile.

3.2.2.1 Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.3 Message Handling Systems

The Message Handling Systems (MHS) Recommendations [CCITT 2-9, CCITT 14, CCITT 28-36] provide message exchange by means of a Message Transfer System consisting of a series of Message Transfer Agents (MTAs) that are responsible for relaying a message from an originator's User Agent (UA) to a recipient's User Agent. A Message Store (MS) can act as an intermediary between the Message Transfer System and the User Agent. A Message Store can submit and accept delivery of messages from the Message Transfer System on behalf of the User Agent as well as perform message storage functions. Off-loading User Agent services to a Message Store allows the configuration of less complex User Agents. The MHS procurement categories are structured to allow users significant flexibility in configuring their systems. The MHS procurement categories vary with the CCITT Recommendations upon which the implementation is based, with the configuration of the Message Handling System, and with the services provided by individual components of the configuration. Users may select several implementations from one procurement category or build their system by selecting implementations from among different procurement categories.

IGOSS Message Handling Systems can be implemented in accordance with either the CCITT 1984 MHS Recommendations or the CCITT 1988 MHS Recommendations.

MHS systems conforming to the CCITT 1988 MHS Recommendations provide significant additional services that are not found in CCITT 1984 MHS implementations. The CCITT 1988 Recommendations also allow users significant flexibility in configuring their systems. Message Transfer Agents, User Agents and Message Stores can be colocated or remote from each other. P3 is the protocol between an MTA and a remote Message Store or User Agent; P7 is the protocol between a remote User Agent and a Message Store. (See fig. 3.2.3.(a)).

These factors result in the following procurement categories for CCITT 1988 MHS implementations. See the Conformance clause of Part 8 of the Workshop Agreements for details on how these configurations relate to the International Standardized Profiles.

"IGOSS1 MHS 1988 MTA" specifies a 1988 relay MTA.

"IGOSS1 MHS 1988 MTA-UA" specifies a 1988 end system in which the MTA is co-located with a CCITT 1988 Interpersonal Messaging (IPM) User Agent, an Electronic Data Interchange (EDI) User Agent or another type of User Agent not standardized by the CCITT.

"IGOSS1 MHS 1988 MTA-MS-UA" specifies an end system in which a Message Store and User Agent are co-located with the MTA.

"IGOSS1 MHS 1988 MTA-MS" specifies an end system in which a Message Store is co-located with the MTA.

"IGOSS1 MHS 1988 Remote UA-MS" specifies a remote User Agent that is co-located with a Message Store.

"IGOSS1 MHS 1988 Remote UA-P3" specifies a remote User Agent that does not require Message Store services.

"IGOSS1 MHS 1988 Remote UA-P7" specifies a remote User Agent that does require Message Store services.

"IGOSS1 MHS 1988 MS" specifies a remote Message Store. The Message Store serves a remote User Agent.

In the procurement categories for CCITT 1988 MHS Implementations, UAs may support one or more of the following: Interpersonal Messaging (IPMS), Electronic Data Interchange (EDI), or any other content type (e.g., Voice Messaging, InterLibrary Loan, Military Messaging (P772), or Message Security Protocol (MSP)). The "S" symbol may optionally be added to indicate that a secure UA is required. The "G" symbol may be added after "MTA" in all procurement categories containing an MTA to indicate that an ADMD gateway cabability is required.

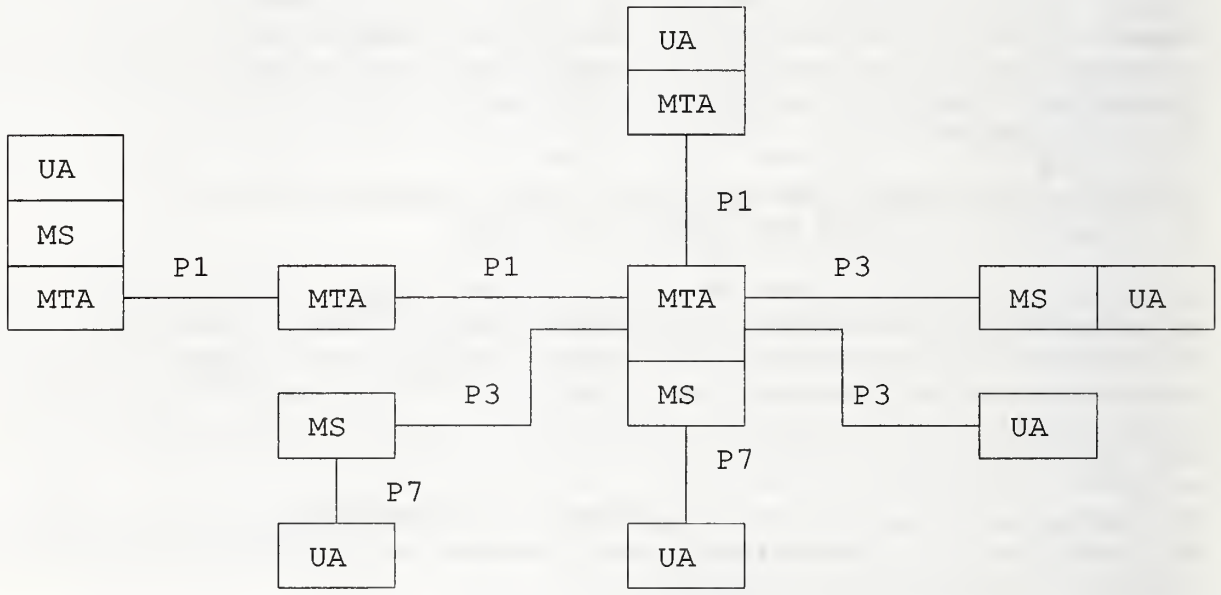


Figure 3.2.3(a). MHS 1988 Configuration Alternatives.

A 1988-based Message Transfer Agent (MTA) must comply with the Common Messaging Message Transfer specification in Part 8 of the Workshop Agreements. This requires support of the 1984 Interworking Functional Group to provide interoperability with CCITT 1984 MHS Implementations by downgrading from the 1988 P1 protocol to the 1984 P1 protocol when relaying from 1988-based to 1984-based MTAs.

Part 8 of the Workshop Agreements specify support for content independent Message Stores or Message Stores supporting specific content types.

All MHS functional entities may access the Directory Service using the Directory User Agent (DUA). An international standard does not yet exist for the interface between these entities and the DUA; thus, the interface is left to either vendor or user definition. When the UA accesses the Directory Service, the Directory name-to-address resolution is performed before message submission. When an MTA accesses

the Directory Service, the Directory name-to-address resolution is performed after the message is submitted. When an address cannot be determined, a non-delivery notification is returned. Part 8, clause 8.4.3 of the Workshop Agreements provides examples of information requests that can be made to a Directory Service using the UA-DUA or MTA-DUA interface.

All Interpersonal Message (IPM) User Agents and all Electronic Data Interchange (EDI) User Agents must be able to access Directory Services using the UA-DUA interface to perform the following functions:

1. Verify the existence of a Directory Name.
2. Return the Originator/Recipient (O/R) Address(es) that correspond to a Directory Name.
3. Determine whether a Directory Name presented denotes a user or a Distribution List.
4. Return the members of a Distribution List.
5. Return the capabilities of the entity referred to by a Directory Name. (e.g., support of particular Body Part)
6. Return the public key or certificate referred to by a Directory Name.

The additional Directory Services functions listed in Part 8, Annex B of the Workshop Agreements are not required, but may be specifically requested by procurement authorities. Access to Directory Services by the Message Transfer System (MTS) is not required, but may be specifically requested by procurement authorities.

ISP AMH1 Part 1 [ISO 111] specifies the Security Functional group as three security classes. Security class S0 implements all security mechanisms outside the MTS (i.e., within the UA or MS). In security class S1, most of the security mechanisms are implemented outside the MTS; however, the MTS provides services related to secure access management. Security class S2 provides authentication and non-repudiation security services within the MTS. Each of the three security classes has a variant, denoted as S0C, S1C and S2C which mandates support of end-to-end confidentiality. Systems implemented in accordance with the CCITT 1988 MHS Recommendation with security services must provide the security services specified in security class S0C. These include integrity of the message content, authentication of the MTS-user who originated the message, authentication of the MTS-user to whom the message was delivered, and content confidentiality. This security class mandates that all services be provided by the MTS-user; there are no security services implemented within the MTS. Additional security services may be requested, if needed, by selecting the appropriate functional groupings from the ISP.

The signing encryption and key management mechanisms used to provide the authentication, integrity and confidentiality security services are beyond the scope of this document. They will be specified in companion documents issued by each IGOSS organization.

Although MHS systems conforming to the CCITT 1988 MHS Recommendations provide significant additional services beyond those specified in the CCITT 1984 Recommendations, procurement categories for CCITT 1984 MHS implementations are included in the IGOSS. This will allow current users of CCITT 1984 MHS implementations, who do not require the additional services available in CCITT 1988 MHS implementations, to add similar systems to their installed base, perhaps at less cost. It should be noted that the Interpersonal Messaging System (IPMs) 1984 Interworking Functional Group insures that all CCITT 1988 MHS implementations will be backwardly compatible for Interpersonal Messaging with CCITT 1984 MHS implementations in the subset of services that they have in common.

Two categories of CCITT 1984 MHS implementations are defined for procurement purposes.

"IGOSS1 MHS 1984 MTA-UA" specifies a 1984 end system in which the MTA is co-located with a CCITT 1984 Interpersonal Messaging (IPM) User Agent. The MTA also has a message relay capability.

"IGOSS1 MHS 1984 MTA" specifies an MTA that functions strictly as a relay MTA.

All IGOSS CCITT 1984 Message Handling Systems must adhere to the agreements for Private Management Domains in Part 7, clause 5 of the Workshop Agreements. All PRMDs must implement and use Transport class 4 and the Connectionless Network Service. CCITT mandates that Administration Domains, which are public message systems operating on public data networks, use Transport class 0 and the Connection Oriented Network Service. PRMD end systems that are also connected to ADMDs must also implement Transport class 0 and the Connection Oriented Network Service when acting as a gateway between the two domains. If an ADMD gateway capability is required, insert "(G)" after "MTA" in both procurement categories listed above.

Figure 3.2.3(b) shows the application subprofile for CCITT 1984 and 1988 MHS implementations. ROSE is required only in those CCITT 1988 MHS configurations in which the Message Store and/or User Agent is remotely located from the MTA. A CCITT 1988 MHS implementation may use either the Reliable Transfer Service (RTS) or RTSE to provide reliable transfer services, but must use the RTS when interoperating with a CCITT 1984 MHS implementation. Application, Presentation and Session Layer support requirements for Message Handling Systems are specified in Part 5, clause 13.2 of the Workshop Agreements.

	MHS (1984)	MHS (1988)		
↑ Application Layer ↓	RTS CCITT X.410	RTS or RTSE ISO 9066-2	ROSE ISO 9072-2	ACSE ISO 8650
Presentation Layer	NULL	ISO 8823		
Session Layer	ISO 8327	ISO 8327		

Figure 3.2.3(b). MHS Application Subprofile.

The CCITT 1988 Recommendations specify the protocol for an Interpersonal Messaging User Agent which provides additional services beyond those provided by the Interpersonal User Agent specified in the CCITT 1984 Recommendations. CCITT Recommendations F.435 [CCITT 46] and X.435 [CCITT 47] specify the services and protocol for an Electronic Data Interchange User Agent. The following subsections reference the agreements that apply to these User Agents.

3.2.3.1 Interpersonal Messaging User Agent

A CCITT 1988 Interpersonal Messaging User Agent must comply with the IPM Service clause of Part 8 of the Workshop Agreements. A CCITT 1984 Interpersonal Messaging User Agent must comply with Part 7, clause 5.3.6 of the Workshop Agreements.

3.2.3.2 Electronic Data Interchange User Agent

An Electronic Data Interchange User Agent provides services related to the exchange of business forms by the MHS application, but independent of the message exchange format (e.g., X12, EDIFACT). An Electronic Data Interchange User Agent interworking with the CCITT 1988 Message Transfer Service must comply with the EDI Messaging service clause of Part 8 of the Workshop Agreements. An Electronic Data

Interchange User Agent can interwork with the CCITT 1984 Message Transfer Service but can not provide the full range of services specified in the CCITT F.435 Recommendation.

3.2.3.3 Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.4 Virtual Terminal - Basic Class

The Virtual Terminal (VT) standard [ISO 32-35] specifies how terminal systems and host applications on a network can communicate without requiring one side to know the terminal characteristics of the other side. The capabilities and constraints of different types of terminal-application dialogues are defined by a virtual terminal profile.

These profiles correspond to the following IGOSS procurement categories for VT systems. A VT system must support one or more of these procurement categories.

"IGOSS1 VT GENERALIZED TELNET"
"IGOSS1 VT FORMS"
"IGOSS1 VT S-MODE PAGED"
"IGOSS1 VT X.3"

The Generalized TELNET profile provides functionality identical to the TELNET protocol of the TCP/IP protocol suite. The Generalized TELNET profile is specified in Part 14, clause 8.5 of the Workshop Agreements.

The Forms profile supports forms-based applications with local entry and validation of data performed by the terminal system. The Forms profile is specified in Part 14, clause 8.3 of the Workshop Agreements.

The S-mode Paged profile provides a forms capability typified by the existing base of block-mode terminals. The S-mode Paged profile is specified by the International Standardized Profile AVT23. [ISO 110]

The X.3 profile provides functionality identical to the set of CCITT recommendations for a Packet Assembler/Disassembler (PAD) (X.3, X.28, X.29). The X.3 profile is specified in Part 14, clause 8.4 of the Workshop Agreements.

Figure 3.2.4 shows the application subprofile for VT implementations. The VT upper layer support requirements are specified in Part 5, clause 13.4 of the Workshop Agreements.

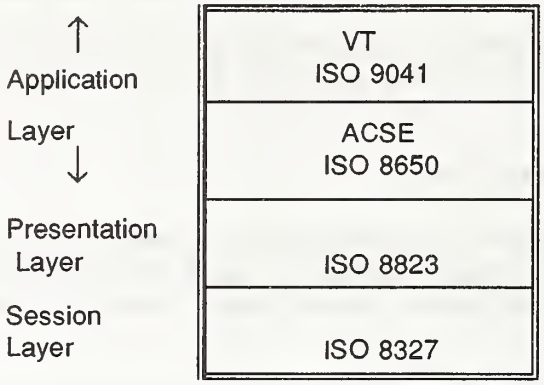


Figure 3.2.4. VT Application Subprofile.

3.2.4.1 Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.5 Transaction Processing

The OSI Transaction Processing (OSI TP) standard [ISO 59-61] and International Standardized Profile (ISP) [ISO 104] support a set of logically related operations affecting interrelated data/resources across separate open systems in which the transaction is not simply an exchange of messages but the exchanges form a protected indivisible set of messages. The ISP augments the standard by specifying the options required to build a conformant TP application. The ISP specifies not only how the TP and Commitment, Concurrency and Recovery (CCR) base standards are used, but also how to construct a conformant Application, Presentation and Session layer. OSI TP operations are characterized by four properties, collectively known as the ACID properties, which guarantee that the results of transactions become visible in a single operation, i.e., all elements of a transaction have the same outcome -- success or failure. The **Atomicity** property states that either all operations are performed or none are performed; the **Consistency** property states that the operations are performed accurately, correctly, and with validity; the **Isolation** property states that partial results of the operations are not externally accessible by operations not involved in the transaction; and the **Durability** property states that the effects of the operations are not altered by any sort of failure, i.e., disk crash after a transaction concludes. The ACID properties are maintained by the CCR standard which is part of the TP ISP [ISO 104].

3.2.5.1 Definitions

1. Transaction Categories:

   A. Application Supported transactions: This category of transaction allows two systems to communicate using a TP Dialogue. The ACID properties are the responsibility of the end user.

B. Provider Supported transactions: This category of transactions allows two systems to communicate using all TP functions. The ACID properties are the responsibility of the TP service provider.

2. Control Modes:

A. Shared Control: This mode does not explicitly control the exchange of messages. Message exchange control is based solely on the internal semantics of the programs and they may use the Dialogue at their discretion. The TP service provider does not care, nor is it aware of any message collisions.

B. Polarized Control: This mode controls the exchange of messages between the two systems via a token. Under normal circumstances a system can use the Dialogue only if it has the token - TP will enforce this. Under extraordinary circumstances, such as an abort, either system can use the Dialogue.

3. Transaction Types:

A. Chained: A chained transaction is a series of related transactions, such as a batch of accounts receivable transactions, which start and continue until the batch ends. The sequence of events is that the first transaction builds the transaction tree, uses it, and either commits or rolls back; the second uses the transaction tree and either commits or rolls back; and the third to the last transaction follow the same pattern. After the last transaction, the transaction tree is disbanded.

B. Unchained: An Unchained transaction establishes a transaction tree and establishes communications with another program. When it is determined that a transaction should occur, that portion of the communication should be placed under the ACID properties and be recoverable by OSI TP. The transaction starts and completes with either a commit or roll back. The transaction tree may be or may not be disbanded. If it remains, it is ready for the next transaction.

C. None (Application Supported): This type of transaction occurs only under the application supported category of transaction. It is an undefined relationship between two systems. How it starts and ends is an end user concern.

4. Roles:

A. Initiator Transaction: In this role a system performs the task of the root node. It starts a transaction and all participants in the transaction are its machines.

B. Responder Transaction: In this role a system may only be a leaf on a transaction tree. It responds to a request to join a transaction and may not delegate any tasks to another system - it can only respond. A large database server might be an example.

C. General Transaction: In this role a system may be a root, intermediate, or leaf node depending on how it is being used at a specific point in time. This is the most robust and general purpose product that could be procured, and can serve in any role.

3.2.5.2. OSI TP Procurement Consideration

This section specifies the OSI TP procurement categories, and the capabilities required of related software.

3.2.5.2.1. OSI TP Procurement Categories

In order to provide interoperability among TP implementations, all IGOSS TP implementations must support the following profiles defined by the TP ISP[ISO 104}:

1. Polarized Application Supported Transactions [ISO 104(a)]
2. Unchained Provider Supported Transactions [ISO 104(b)], and
3. Chained Provider Supported Transactions [ISO 104(c)].

TP systems must support one of the following procurement categories.

"IGOSS1 TP (I)"
"IGOSS1 TP (R)"
"IGOSS1 TP (G)"

where x = I (Initiator role only), R (Responder role only, or G (General role-both Initiator and Responder).

Products that can operate in a general role are the most robust and should be procured wherever possible. Products that can operate only in an Initiator or Responder role should be procured only when the additional services will never be required and the cost savings make up for the loss of flexibility. Single role products can also be procured when the underlying platform will not support a General role product.

A specific TP product may provide more functionality than the minimum required for the application. This should be viewed as a plus because it offers greater flexibility and possibly lower life cycle costs as the application changes to meet new user requirements.

OSI TP systems in all procurement categories are bound by the language and conditions contained in Part 15 of the Workshop Agreements.

Figure 3.2.5.2.1 shows the application subprofile for OSI TP implementations. The upper layer support requirements for OSI TP are specified in Part 5, clause 13.6 of the Workshop Agreements.

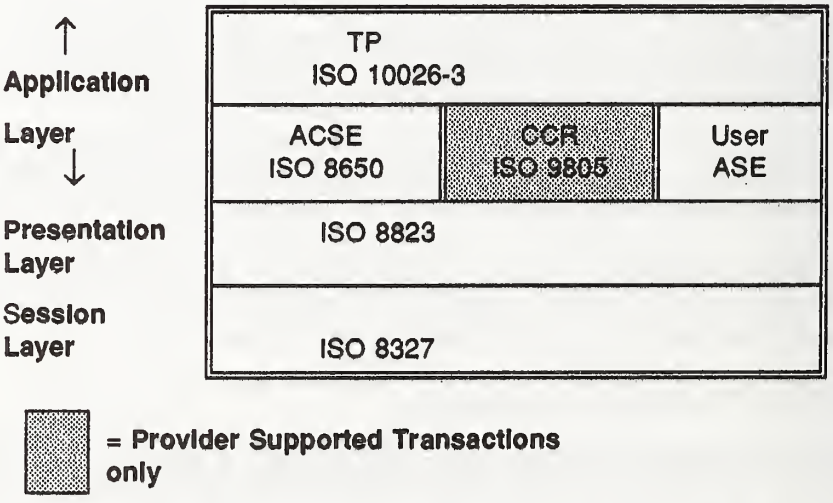


Figure 3.2.5.2.1. OSI TP Application Subprofile.

3.2.5.2.2. Transaction Processing Formats

This section specifies the format of certain Transaction Processing data elements.

3.2.5.2.2.1. Transaction Processing Service Unit (TPSU)-Title

The TPSU-Title format is the T61-String. This is a 1..64 octet string.

3.2.5.2.2.2. Application Entity (AE)-Title

For the local generation of AE-Titles, IGOSS only requires support for AE-Title-Form-2 (Object id) which is the form mandatory in the TP ISP [ISO 104]. An intermediate mode must also be able to propagate AE-Title-Form-1 (directory form).

3.2.5.2.3. Related software

When procuring TP systems it is important to remember that related software, such as database management systems, must be able to interoperate with them. These products must be able to interact with such things as TP's two-phase commit, and recovery mechanisms.

Of special concern, is how these products transmit program aborts. The user program can take responsibility for transmitting that information to the service provider or the vendor product can interact directly with the TP product. The more integrated the related vendor product is with OSI TP, the better the product is.

3.2.5.2.3.1. Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such, it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.6 Remote Database Access

The Remote Database Access (RDA) standard provides protocols for establishing a remote connection between a database client and a database server. The RDA standard addresses distributed database processing in this client/server environment. RDA specifies a two-way transfer syntax and, when combined with a database specialization, semantics for database operations.

The RDA standard is specified in two parts. Part 1 [ISO 62] defines the RDA Generic Model, Service, and Protocol. Part 2 [ISO 63] defines the RDA Structured Query Language (SQL) Specialization. RDA conformance can only be expressed in conjunction with a specific database language. The RDA SQL Specialization allows the connection of RDA clients with RDA servers conforming to database language SQL [ISO 68]. Both the client and the server must conform to the RDA SQL Specialization protocol; however, only the server need provide an SQL conformant client database management system. The client can be an application that simply sends SQL statements to the server. SQL is thus far the only specialization developed to complement the RDA Generic Model, Service and Protocol.

An RDA application may be implemented in conjunction with the Basic Application Context or the TP Application Context. The Basic Application Context includes only the ACSE Application Service Element and provides a one-phase commit protocol. The TP Application Context provides a two-phase commit which allows updates at multiple remote sites in the same transaction. Initial RDA implementations will use

the Basic Application Context. Procurement categories for the TP Application Context will be specified in a later version of the IGOSS.

IGOSS specifies four procurement categories for RDA Basic Application Context implementations.

"IGOSS1 RDA BASIC IMMEDIATE EXECUTION" immediately executes the database operation.

"IGOSS1 RDA BASIC STORED EXECUTION" permits optimization by allowing database operations to be defined and stored at the database server and to be executed one or more times during the RDA dialogue possible with different parameters for each execution.

"IGOSS1 RDA BASIC STATUS" allows the status of a database operation to be queried.

"IGOSS1 RDA BASIC CANCEL" allows a database operation to be cancelled.

Only the first procurement category is required for IGOSS RDA profile conformance. The other categories are supersets of the first category, but not supersets of each other. If the optional services required by these categories are required, more than one procurement category must be selected. RDA implementations in all categories are bound by the language and conditions contained in Part 19 of the Workshop Agreements.

Figure 3.2.6 shows the application subprofile for RDA implementations. The upper layer support requirements for RDA are specified in Part 5, clause 13.8 of the Workshop Agreements.

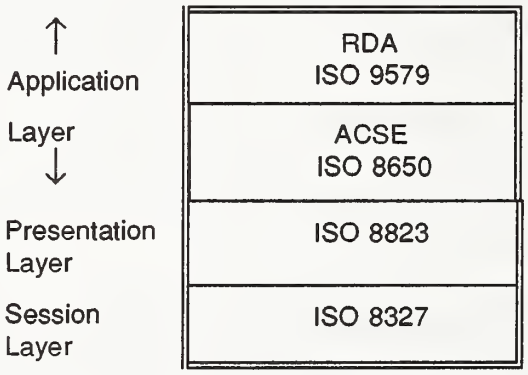


Figure 3.2.6. RDA Basic Application Context Application Subprofile.

3.2.6.1. Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the connection oriented transport service. As such it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.7 Directory Services

The Directory Service application provides access to a collection of information about objects of interest to OSI users. The information is found in a Directory Information Base (sometimes called the Directory Information Tree, or DIT). The Directory Service is based on a standard produced in collaboration between CCITT [CCITT 37-45] and ISO/IEC [ISO 70-78]. The first edition (1988) was extended to provide several

new features of functionality including standardized mechanisms for access control and replication (1993 edition). This specification is based entirely on the 1993 edition of the Directory Standard. The Directory Service, provided by a potentially distributed system of Directory Service Agents (DSAs), is accessed by invoking a functional component known as a Directory User Agent (DUA). When a DUA conveys a request to a DSA and a DSA responds, the Directory Access Protocol (DAP) is used. If the DSA contacted by the DUA cannot process the request, it may propagate or "chain" the request to another DSA which may repeat the chaining operation, or the initial DSA may provide the DUA with a "referral" to another DSA more likely to contain the information. The protocol used among DSAs to convey a service request or response is known as the Directory System Protocol (DSP). When DSAs replicate information to enhance availability and performance, two other protocols are used. The Directory Operational Binding Management Protocol (DOP) can optionally be used to initialize or terminate a relationship between two DSAs regarding the supply and consumption of replicated information and regarding the distribution of knowledge regarding the content of DSAs. The Directory Information Shadowing Protocol (DISP) is used to initially provide and to refresh replicated information. Figure 3.2.7 shows the application subprofile for Directory Service implementations.

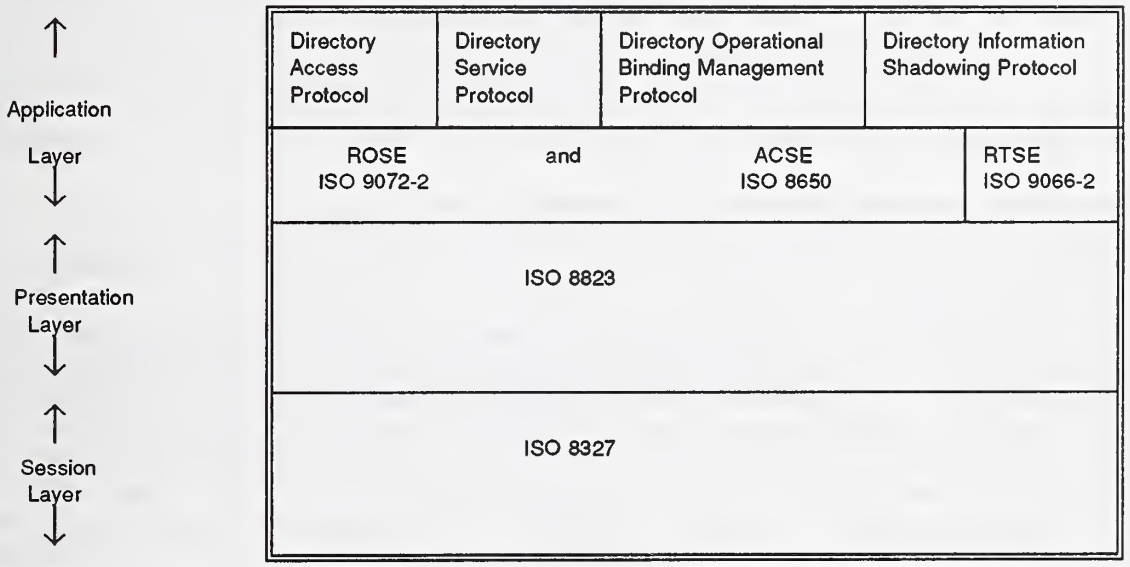


Figure 3.2.7. Directory Service Application Subprofile.

3.2.7.1 Directory User Agent Procurement Categories

IGOSS procurement categories for DUAs use three dimensions to specify required functionality:

1. supported abstract operations;
2. supported types and levels of authentication; and
3. ability to use a Continuation Reference to progress an operation.

3.2.7.1.1 DUA: Supported Abstract Operations

The OSI Directory standard allows DUAs to support one, several, or all abstract operations defined for the Directory Access Protocol (DAP). A complete list of the DAP abstract operations is given in Table 3.1. These operation names will be printed in bold type in this document.

For convenience, the IGOSS procurement classifications provide three "bundles" of DUA functionality as follows.

1. A "Lookup" DUA supports the **Read** operation only.
2. A "Browse" DUA supports the **Read, Compare, List, Search**, and **Abandon** operations only.
3. An "Administrative" DUA supports all DAP abstract operations.

Table 3.1 Directory DAP Abstract Operations

o **Read**	o **RemoveEntry**
o **Compare**	o **ModifyEntry**
o **List**	o **ModifyDN**
o **Search**	o **Abandon**
o **AddEntry**	

Certain 1993 extensions to the abstract operations specified in Appendix 6 must also be supported.

3.2.7.1.2 DUA: Supported Types and Levels of Authentication

The OSI Directory standard accommodates two basic types of authentication - user authentication and peer-entity authentication - and three security levels at which authentication may be performed: identity-only, simple, and strong. Authentication based on identity-only provides no real confidence that the identity presented to the Directory is authentic. Authentication based on unprotected passwords is not sufficient to satisfy a requirement for simple authentication. Simple authentication is based on protected passwords and may, depending on how the passwords are administered and protected, provide more confidence than identity-only authentication. The standard allows a password to be either protected or unprotected from disclosure as it is transmitted from the DUA to a DSA. A password is protected through the use of a secure one-way hash function. An IGOSS conformant DUA shall, at a minimum, support identity-only and simple authentication. These services are provided by Authentication Modes 0 and 1 as specified in Appendix 6 of this document.

Strong authentication is based on the use of digital signatures which, in turn, rely on the use of public key cryptographic techniques. Such techniques require the generation and management of public and private key material. Management of public key material involves the use of a Certification Authority (as described in [CCITT 39]) which is responsible for digitally signing certificates held in the Directory and used to verify digital signatures. Management of the private key material involves maintaining its confidentiality as it is communicated between the source that generated the key and the user associated with the key. Generation of the public and private key material involves ensuring that the keys have specific mathematical qualities. The Certification Authority may be responsible for generating keys with the required qualities. Certification Authorities also provide the basis for trusted paths (within the Directory Information Tree (DIT)) of certification as described in [CCITT 39]. These trusted paths are used in verifying a digital signature when the user community involves more than one Certification Authority. The details of procuring Certificate Authority service are outside the scope of this specification; however, there are two choices for obtaining such a service: buy the service from a commercial Certification Authority or procure the necessary equipment and expertise to provide the service in-house.

The IGOSS provides three categories of strong authentication which are specified by Enhanced Authentication Modes 2-4 in Appendix 6 of this document. These Enhanced Authentication Modes enable a DUA to transmit credentials which will allow a DUA to perform strong authentication at the time the DAP connection is established or when an individual abstract operation is invoked as well as to perform strong authentication based on credentials transmitted by the DSA.

The digital signature and secure one-way hash algorithms used in authentication services are beyond the scope of this document. They will be specified in companion documents issued by each IGOSS organization.

3.2.7.1.3 DUA: Support For Resolution of Continuation Reference

A DUA may receive a ContinuationReference as part of a **List** or **Search** result. A DUA might also receive a continuation reference when a DSA responds to an operation by issuing a referral to another DSA.

Some DUAs may be designed for use in environments where such references are never used, or a DUA may be simplified such that it cannot pursue a reference. Alternatively, a DUA may be designed to be capable of pursuing references. Another possibility is that a DUA product is designed to be configurable such that the capability to pursue references may be controlled (either by the user or by the system administrator). The following Reference Resolution Modes are used in the IGOSS to specify this dimension of a DUA.

- Reference Resolution Mode 0: Reference Resolution Mode 0 is used to specify a DUA that is not capable of using a continuation reference to redirect an operation to the DSA indicated in the reference.

- Reference Resolution Mode 1: Reference Resolution Mode 1 is supported by a DUA that is capable of using a continuation reference to redirect an operation to the DSA indicated in the reference. A DUA that supports this mode shall detect reference loops. A DUA that supports this mode shall be configurable to allow the user (or, alternatively, the system administrator) to disable reference resolution.

3.2.7.1.4 DUA Procurement Classes

An IGOSS procurement class, used to specify DUA product requirements, is formed by specifying three parameters as follows.

1. The first parameter specifies whether the DUA is Lookup, Browse, or Administrative.

2. The second parameter specifies the Enhanced Authentication Modes (beyond those mandated by IGOSS) that must be supported by the DUA. This parameter is not required if strong authentication services are not required. An IGOSS conformant DUA shall, at a minimum, support Authentication modes 0 and 1.

3. The third parameter specifies which Reference Resolution Mode is supported by the DUA.

Labels for DUA procurement classes are of the form:

"IGOSS1 DS 1993 DUA, Operations(X), Enhanced Authentication Modes(Y), Reference Resolution Mode(Z)"

where

X is "Lookup" or "Browse" or "Administrative" and

Y is a list of required Authentication Modes (may be omitted if no enhanced authentication modes are required) other than modes 0 and 1, and

Z specifies the required Reference Resolution Mode as either 0 or 1.

3.2.7.2 Directory System Agent Procurement Categories

IGOSS procurement categories for DSA products are based on:

1. DSA category; and
2. supported types and levels of authentication.

3.2.7.2.1 DSA Product Categories

The DSA product taxonomy has two basic categories. The first category, referred to as "solitary," is a DSA designed to support a centralized DIT only and is unable to communicate with any other DSA. The second category, referred to as "cooperative," is used to specify a bundle of functionality that allows a DSA to be part of a community of DSAs which communicate in various ways to support a distributed DIT.

A solitary DSA never communicates with any other DSA and hence does not support DSP, DISP, DOP, referrals, and knowledge references. When specifying a solitary DSA it is necessary to address requirements for extensions to abstract operations, authentication, and access control.

A cooperative DSA is able to cooperate, either directly or indirectly, with other DSAs to provide Directory services which are, to a large extent, independent of how the DIT is distributed. Cooperation can occur directly when a DSA supports the DSP as both a responder and an initiator, and therefore supports the chained mode of operation. Cooperation can occur indirectly when a DSA supports DAP only or when only the responder role for DSP is supported. An indirectly-cooperative DSA generally returns referrals when its local fragment of the DIT is insufficient to complete an operation result.

Table 3.2 DSA Categories

DESCRIPTION OF PRODUCT CLASS	TAXONOMIC LABEL
Solitary.....	solitary
Cooperative	
Capable of chaining	
accessible by DSA only.....	chainer - indirect access
accessible by DUA and DSA.....	chainer - full access
Not capable of chaining	
accessible by DUA only	nonchainer - direct access
accessible by DSA only	nonchainer - indirect access
accessible by DUA and DSA	nonchainer - full access

There are, therefore, two subclasses of cooperative DSA: directly cooperative (referred to as a "chaining" DSA), and indirectly cooperative (referred to as a "nonchaining" DSA). These subclasses, in turn, have subclasses based on whether the DSA is accessible by a DUA only, a DSA only, or by both DUA and DSA. A chaining DSA may or may not be capable of communicating with a DUA. A nonchaining DSA may communicate with DUAs only or with DSAs only or may be capable of communicating with both. These subclasses are summarized and labeled in Table 3.2.

3.2.7.2.2 DSA: Supported Types and Levels of Authentication

Authentication Modes associated with DUA - DSA interaction are compatible with the DUA Authentication Modes discussed in Section 3.2.7.1.2. For example, a DUA supporting Authentication Modes 0 and 1 can be used with a DSA that supports Authentication Modes 0 and 1. Additional DSA Authenication Modes are used to perform peer-entity authentication in a chained transaction. These Authentication Modes are fully specified in Appendix 6 of this document. Appendix 6 also specifies additional conformance requirements for IGOSS DSAs.

The digital signature and secure one-way hash algorithms used in authentication services are beyond the scope of this document; they will be specified in companion documents issued by each IGOSS organization.

3.2.7.2.3 Labels for DSA Procurement Classes

Labels for DSA procurement classes are of the form:

"IGOSS1 DS 1993 DSA, Category(X), Authentication Modes(Y)"

where

X is one of the following:

"solitary"
"chainer -- indirect access"
"chainer -- full access"
"nonchainer -- direct access"
"nonchainer -- indirect access"
"nonchainer -- full access"

Y is a list of the Authentication Modes, required by the acquisition authority, subject to the following constraints:

1. For solitary DSAs, the list may the list may contain any combination of modes 0 through 5.

2. For "chainer -- indirect access" DSAs, the list may contain any combination of modes 3 through 7.

3. For "chainer -- full access" DSAs, the list may contain any combination of modes 0 through 7.

4. For "nonchainer -- indirect access" DSAs, the list may contain any combination of modes 3, 4, 5, and 7.

5. For "nonchainer -- direct access" and "nonchainer -- full access" DSAs, the list may contain any combination of modes 0, 1, 2, 3, 4, 5, 7.

3.2.7.3 Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such, it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.8 Manufacturing Message Specification

The Manufacturing Message Specification (MMS) standard [ISO 64-65] provides for client/server message based communications between programmable devices in a computer controlled environment. MMS must be implemented as specified in Part 20 of the Workshop Agreements.

There is an installed base of real implementations based on the Draft International Standard (DIS). If backward compatibility with existing devices supporting the MMS DIS protocol is necessary, the acquisition authority should require implementations to support the agreements found in Part 20, Annex A of the Workshop Agreements document .

MMS defines messages useful for information interchange. It does not define a complete set of services for remote device programming.

The MMS standard uses the terms client and server. The client is the system that that requests provision of a service. The server is the provider of the requested service. Server behaviors and allowable responses are well defined in the MMS standard. Client and server roles are MMS service specific. A device may support some services in a client role, other services in a server role, and still other services in both the client and server roles.

The MMS standard defines 86 different messaging services. Implementations conforming to the MMS standard must support five mandatory MMS services (Initiate, Conclude, Abort, Reject, and Identify). Implementation support for any of the other MMS services is optional.

While it is unlikely that any device would support all of the MMS services, experience has shown that there are MMS service groupings that meet the current functional application needs of real manufacturing devices. These useful MMS service groupings are called implementation classes.

Eight MMS implementation classes are specified in the following tables (Table 3.3 and Table 3.4). MMS implementation classes are closely allgned with the correspondlngly numbered MMS implementation classes found in the MAP 3.0 specification. All IGOSS MMS implementations must support MMS implementation class 0 plus one or more additional MMS implementation classes. These MMS implementation classes equate to IGOSS procurement classes **"IGOSS1 MMS 1-7."** MMS implementation class 0 is intended to be consistent with the proposed first MMS general application ISP.

The following conventions are used in the Implementation Class/Service Table (Table 3.3).

LETTER "Y"

In the Implementation Class/Service table, a "y" indicates that the implementation shall support both the Server and Client Conformance requirements for these services.

LETTER "X"

In the Implementation Class/Service table, an "x" indicates that the service shall be included in the Implementation Class. For services contained in an implementation class, the implementation shall support either all Client conformance requirements for the services or all Server conformance requirements for the services.

LETTER "A" AND LETTER "B"

In the Implementation Class/Service table, wherever A and B are specified within a given Implementation Class, the implementation is required to support either all A services or all B services in that Implementation Class. For services contained in an implementation class, the implementation shall support either all Client conformance requirements for the services or all Server conformance requirements for the services.

Table 3.3 MMS Implementation Class/Service Mapping

SERVICE	IMPLEMENTATION CLASS							
	0	1	2	3	4	5	6	7
Initiate	X	Y	Y	Y	Y	X	Y	Y
Conclude	X	Y	Y	Y	Y	X	Y	Y
Cancel			X	X	X	X	X	X
Reject	X	Y	Y	Y	Y	X	Y	Y
Abort	X	Y	Y	Y	Y	X	Y	Y
Status		X	X	X	X	X	X	X
GetNameList		X	X	X	X	X	X	X
Identify	X	X	X	X	X	X	X	X
UnsolicitedStatus		X		X	X			
GetCapabilityList		X	X	X	X	X	X	X
InitiateDownloadSequence		A		X	A	A	A	A
DownloadSegment		A		X	A	A	A	A
TerminateDownloadSequence		A		X	A	A	A	A
InitiateUploadSequence		A		X	A	A	A	A
UploadSegment		A		X	A	A	A	A
TerminateUploadSequence		A		X	A	A	A	A
RequestDomainDownload		A			A			
RequestDomainUpload		A			A			
LoadDomainContent		B			B	B	B	B
StoreDomainContent		B			B	B	B	B

Table 3.3 MMS Implementation Class/Service Mapping (cont'd)

SERVICE	IMPLEMENTATION CLASS						
	1	2	3	4	5	6	7
DeleteDomain			X	X			
GetDomainAttributes			X	X	X	X	X
CreateProgramInvocation	X		X	X			
DeleteProgramInvocation	X		X	X			
Start	X		X	X			X
Stop	X		X	X			X
Resume	X		X	X			X
Reset			X	X			X
Kill							X
GetProgramInvocationAttributes			X	X			X
Read	X	X	X	X	X	X	X
Write	X	X	X	X	X	X	X
InformationReport	X			X			
GetVariableAccessAttributes		X	X	X			
TakeControl				X	X	X	X
RelinquishControl				X	X	X	X
ReportSemaphoreStatus				X	X	X	X

Table 3.3 MMS Implementation Class/Service Mapping (cont'd)

SERVICE	IMPLEMENTATION CLASS						
	1	2	3	4	5	6	7
ReportPoolSemaphoreStatus				X	X	X	X
ReportSemaphoreEntryStatus				X	X	X	X
Input	X			X			
Output	X			X			
GetEventConditionAttributes					X	X	X
ReportEventConditionStatus					X	X	X
GetAlarmSummary					X	X	X
ReadJournal						X	X
WriteJournal						X	X
InitializeJournal						X	X
CreateJournal						X	X
DeleteJournal						X	X
ReportJournalStatus						X	X
ObtainFile	B			B			

The following conventions are used in the Implementation Class/Parameter Table (Table 3.4) which indicates the parameter support required for each MMS implementation class.

Letter "X":

In the Implementation Class/Parameter table, an "X" indicates that the parameter shall be included in the Implementation Class.

Letter "C" and Letter "D":

In the Implementation Class/Parameter table, wherever C and D are specified the implementation is required to support either the C or D parameter.

Table 3.4 MMS Implementation Class/Parameter

Parameter	Implementation Class						
	1	2	3	4	5	6	7
STR1	X		X	X			
STR2							
NEST	1	0	1	1	0	0	0
VNAM	X	C	X	X	X	X	X
VADR		D					
VALT							
VSCA							
TPY							

Figure 3.2.8 shows the application subprofile for MMS implementations. The upper layer support requirements for MMS are specified in Part 5, clause 13.5 of the Workshop Agreements.

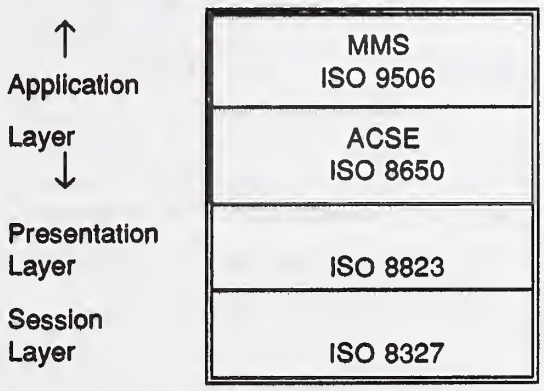


Figure 3.2.8. MMS Application Subprofile.

3.2.8.1 Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such, it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.9 Network Management

Network management is provided by a family of standards covering the areas of management communications, management information, and systems management functions and services. The single procurement category of network management systems is "IGOSS1 NM." An IGOSS1 NM implementation shall be conformant to all three areas as specified in Section 3.2.9.1 - 3.2.9.3. If management security is required, an implementation shall support one of the two peer-entity authentication modes as described in Section 3.2.9.4; inclusion of the security feature is optional.

When procuring a complete Network Management System, the acquisition authority should take additional steps to ensure an adequate specification for the intended use.

3.2.9.1 Management Communications

To be conformant in the area of management communications, an implementation shall satisfy the requirements for management communications as stated in Part 18, clause 8.3.1 of the Workshop Agreements. These agreements relate to the Common Management Information Services (CMIS) [ISO 79] and the Common Management Information Protocol (CMIP) [ISO 80]. Figure 3.2.9.2 shows the CMIP application subprofile. Upper Layer support requirements for Network Management are specified in Part 5, clause 13.7 of the Workshop Agreements.

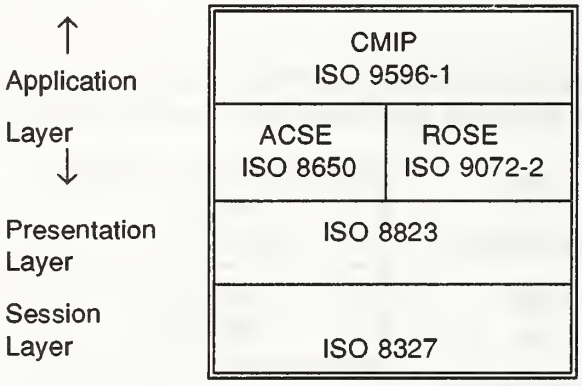


Figure 3.2.9.2. Network Management Application Subprofile.

3.2.9.2 Management Information

To provide interoperability among network management systems, each system must have a common "view" of management information. A system supporting the IGOSS NM application subprofile shall also support OSI management information for its lower layer subprofiles (Transport and Network layers) (see sec. 3.4.4). Where applicable, additional managed objects may be selected from the MO definitions in the following documents:

- o DMI [ISO 81]
- o Annex A and B of Part 18 (NM IAs) of the Workshop Agreements [NIST 1]
- o IEEE 802.1B LAN/MAN Management [IEEE 4]
- o IEEE 802.3 Repeater Management [IEEE 5]
- o ANSI X3T9.5 FDDI Station Management [ISO 99]
- o CCITT Generic Network Information Model [CCITT 48]
- o The Network Management Forum Management Information Library [MISC 9]

When specifying MOs for NM products, the acquisition authority must take care to specify: 1) from which document the MOs are selected, since MO names need only be unique within a particular defining document and may, therefore, be similar or identical to names of different objects in other documents; 2) whether, and which, optional attributes and/or conditional package(s) are mandatory for the procurement; and 3) at least one name binding for each of the MOs selected.

In those cases where applicable MOs cannot be found in the above listed documents for managing particular network component(s) or system(s), additional, more appropriate managed objects may need to be defined. The definitions of such managed objects must satisfy the requirements for management information as stated in Part 18, clause 8.3.3 of the Workshop Agreements. The techniques and templates specified in [ISO 85] must be used in defining these MOs. When defining these MOs, two steps must be taken to assure that the management information base is kept as lean and coherent as possible. First, the management information documents listed above, plus those SMFs identified in Section 3.2.9.3 should be thoroughly searched to assure that an appropriate MO has not already been defined for the desired purpose. Then, these same documents should be searched for an already defined MO which, although not entirely satisfactory, may be sufficiently close to the desired MO so that it could serve as a superior object class from which this new object class could be derived. Elements of MOs (e.g., attributes or notifications) should be handled in the same manner to prevent redundant definition of similar or identical management information elements. All MO definitions must have registered object identifiers and must be publicly available.

3.2.9.3 System Management Functions and Services

To develop functions for the support of systems management, standards groups have partitioned systems management activities into five Specific Management Functional Areas (SMFAs): configuration management, fault management, performance management, security management, and accounting management. Within each of these SMFAs, standards groups are developing standards for functions (including requirements, models, and services) for the management of networks. Because of overlap among requirements of the SMFAs, management functions developed to satisfy the needs of one SMFA can often be used in support of other SMFAs. The functions are known as Systems Management Functions (SMFs). Seven of these SMFs are included in this version of IGOSS: Object Management Function (OMF) [ISO 86], State Management Function (STMF) [ISO 87], Attributes for Representing Relationships (ARR) [ISO 88], Alarm Reporting Function (ARF) [ISO 89], Event Report Management Function (ERMF) [ISO 90], Log Control Function (LCF) [ISO 91], and Security Alarm Reporting Function (SARF) [ISO 92].

To be conformant in the area of systems management functions, an implementation shall satisfy the requirements for systems management functions as stated in Part 18, clause 8.3.2 of the Workshop Agreements.

As specified in Part 18, clause 8.3.2 of the Workshop Agreements when specifying systems management functions (SMF) for NM products, the acquisition authority should take care to select the applicable SMF categories. The SMF categories include:

- General Management Capabilities,
- Alarm Reporting and State Management Capabilities,
- Alarm Reporting Capabilities,
- General Event Report Management Capabilities, and
- General Log Control Capabilities.

The acquisition authority, when specifying the selected SMF categories shall also specify the selected functional units and shall specify whether conformance to the agent role, the manager role, or both, is required.

3.2.9.4 Management Security

To accommodate current management security needs prior to standards reaching full maturity, there are two modes of authentication between which acquisition authorities may choose. Specification of security requirements is optional. If required, the acquisition authority shall select only one of the two modes of authentication. It is strongly recommended that the acquisition authorities requiring the optional authentication service specify Mode 2.

Both modes use simple credentials, as defined in the Directory Authentication standard [ISO 77], to authenticate an entity requesting the establishment of a management association. The simple credentials structure comprises the following fields: username, password, optional time-stamp, and random number fields. The time-stamp fields and random number fields may be used to protect against replay attacks.

Mode 1: Mode 1 authentication requires use of the username and password fields of the simple credentials. This method uses the ACSE Authentication Service/Protocol [ISO 93-94] which defines a new functional unit (authentication) in which this information is conveyed in the protocol data unit (PDU). An authenticating entity must compare the username and password against an "authorized users" list to verify the user's identity. If the identity is confirmed, the association is accepted; otherwise, it is rejected. The username and password are the minimum amount of information that must be provided for Mode 1 authentication. The password is transmitted in the clear, not encrypted in any way. Distribution methods for the usernames and passwords are dependent upon prior agreements between communicating peer entities, and are, therefore, beyond the scope of this version of the IGOSS.

Mode 2: In addition to providing all aspects of Mode 1 authentication, Mode 2 authentication provides additional security by using a hash function applied to the authentication information (i.e., the password). Optional fields (e.g., the time-stamp or random number field) may be included in the authentication information, to which the hash function is applied, to provide a greater measure of security (i.e., by adding the time-stamp, the password will hash to a different value each time). The recommended hash function to be used in Mode 2 authentication is the Secure Hash Algorithm (SHA) as specified in [NIST 14]; additional hash functions may be specified in companion documents issued by individual IGOSS organizatons. The authenticating entity receives the hashed output in the password field of the simple credentials structure, and then processes the password "known" locally to correspond to the received username (along with the other authentication information as the requesting entity ID) using the hash function to produce a test value. This test value and the password field are then checked for equality. If the user identity is authenticated, the association is accepted; otherwise, it is rejected. The distribution of the actual password used as input for hashing is dependent upon prior agreements between communicating peer entities, and is, therefore, not part of this specification.

Once authenticated on an association, an entity shall have access to all management information available through that association. If an entity is not authenticated, it will not be granted an association.

3.2.9.4.1 Requirements for Combination with Specific Lower Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such, it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.9.5 Relationship of IGOSS Network Management to Other Efforts

The Open Management Roadmap, an international partnership of government and industry, vendors and users, is an endeavor, initiated and managed by the Network Management Forum (NMF), to coordinate all the related network management activities of developing standards and defining specifications to produce interoperable network management products. Currently, the partnership includes: CCTA (UK Government Center for Information Systems), European Community Testing Service for Network Management (CTS3/NM), National Institute of Standards and Technology (NIST), Network Management Forum (NMF), X/OPEN, Object Management Group (OMG), the Open Software Foundation (OSF), Corporation for Open Systems (COS), Interoperability Technology Association for Information Processing (INTAP), Standards Promotion and Application Group (SPAG), UI (UNIX International), and the User Advisory Council (UAC). Standards organizations and regional workshops, such as the OIW, are source organizations in the Roadmap activity.

The Roadmap partnership agreed to a plan for defining a number of Open Management Interoperability Points (OMNI*Points*) which are snapshots of standards, specifications, and agreements for network management. At each OMNIPoint, a set of specifications is to be published to which the vendor partners agree to develop products and for which the user partners expect to purchase products.

The first OMNI*Point* specification, released in October 1992, includes Version 1 of the Government Network Management Profile (GNMP) [NIST 4] as an example procurement document whose requirements may be met by OP1 products. In other words, V.1 GNMP is a subset of OMNIPoint1.

Network Management (NM) for IGOSS is compatible with Version 1 of the GNMP except that the IGOSS requires that all the management information defined by the ISO/IEC JTC1/SC6 for the OSI Transport, and Network Layer Standards be supported, and all three NM areas as specified in Section 3.2.9.5 - 3.2.9.3 be supported. V.1 GNMP-conformant products must implement one or more of these areas and implementation of the management information defined by the ISO JTC1/SC6 for the Transport and the Network Layer Standards are optional.

Continued collaboration and participation in the Open Management Roadmap by IGOSS organizations is expected as the IGOSS and GNMP evolves and additional OMNIPoints are defined.

3.2.10 X-Windows

X-Windows is a graphical user interface standard which enables a user to view and gain access to multiple computer applications from a single window or multiple windows on a display screen. X-Windows is based on a client/server architecture which allows applications and resources to be distributed across a network. The X-server is a software program that is resident on a user's display unit that acts as an intermediary between the user and applications running on a local or remote system. The applications are referred to as X-clients. These applications access the display unit by sending messages to the X-server which is then able to perform the two dimensional drawing of lines, shapes and text. The X-server also maintains complex data structures such as specific windows, cursors and fonts which can be referenced and utilized by applications. Input from the keyboard and/or mouse is collected by the X-server and passed to local and/or remote applications for processing.

X-windows products are based on a specification [MISC 7] which is a de facto standard maintained by the X Consortium. However, this specification does not provide for running X-windows over OSI-based networks. To run X-windows over OSI, the mapping of X-windows onto a mOSI compliant stack defined in Part 14, Annex D of the OIW Agreements is required. Interoperability is ensured for implementations of X-windows over OSI following this mapping.

When procuring X-Windows clients and servers, the acquisition authority shall also require

a) an OSI stack providing mOSI (see sec. 3.2.13) compliant services (which provides an OSI transport mechanism for X-Windows) as defined in Part 14, Annex D of the Workshop Agreements, and

b) a protocol such as that specified in the VT Generalized Telnet profile (See sec. 3.2.4) that will allow remote clients to be initiated in an OSI environment.

The procurement categories that apply to the procurement of an X-Windows application operating over an OSI-based network is:

"IGOSS1 X-W (C)"
"IGOSS1 X-W (S)"
"IGOSS1 X-W (CS)"

where "C"= Client, "S"= Server and "CS"= both

Figure 3.2.10 shows the application subprofile for X-Windows OSI implementations.

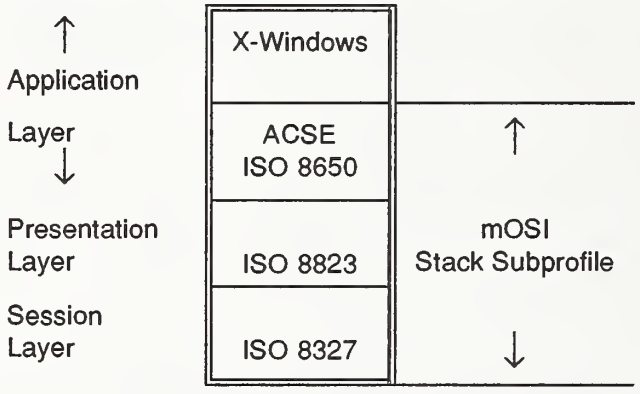


Figure 3.2.10. X-Windows Application Subprofile.

3.2.10.1 Requirements for Combination with Specific Upper Layer Subprofiles

This application subprofile requires the use of the minimal OSI (mOSI) upper layer service. As such it must be combined with the mOSI upper layer service subprofiles to define a complete procurement.

3.2.11 Information Retrieval

The Information Retrieval (IR) application supports the open interconnection of information clients with information servers by specifying an OSI application layer protocol for intersystem search and retrieval of information. IR addresses retrieval (but not update) of information and the IR protocol specifies basic information retrieval operations, a common syntax for queries and the means to express their semantics, and the means to allow the partner systems to share an understanding of the information retrieved.

The IR protocol provides access to information resorces without requiring servers to structure databases similarly, or name fields within record structures similarly. It provides the means to register attribute set definitions that express the semantics of information exchanged. The standard supplies a basic attribute set for search and retrieval of text-based information.

The protocol may be based on the international standard [ISO 66-67] or the national standard [ANSI 7] which is a compatible superset of the international standard. The national standard has a proximity searching feature plus access control and resource control services that have not yet been incorporated into the international standard. A negotiation of the services to be provided, which occurs during the initialization of the association, allows implementations conforming to the two standards to interoperate. Functional profiles have been defined that correspond to both the international [ISO 69] and national [MISC 8] standards. The standards and functional profiles correspond to the following IGOSS procurement categories for IR systems:

"IGOSS1 IR ISO (C)"
"IGOSS1 IR ISO (S)"
"IGOSS1 IR ISO (CS)"
"IGOSS1 IR ANSI (C)"
"IGOSS1 IR ANSI (S)"
"IGOSS1 IR ANSI (CS)"

where "C"= client, "S"= server and "CS"= both

Figure 3.2.11 shows the application subprofile for IR systems. The IR upper layer support requirements include the kernel functional units of ACSE, the Presentation Layer and the Session Layer, plus the duplex functional unit of the Session layer.

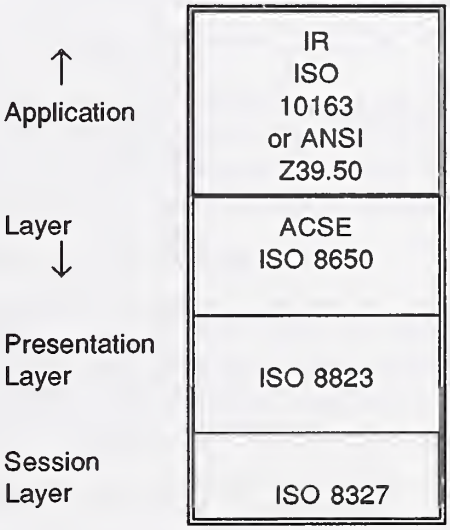


Figure 3.2.11. IR Application Subprofile.

3.2.11.1 Requirements for Combination with Specific Upper Layer Subprofiles

This application subprofile requires the use of the Connection Oriented Transport Service. As such, it may be combined with either the COTS-CLNS or COTS(X)-CONS lower layer subprofiles to define a complete procurement.

3.2.12 OSI Upper Layer Connectionless Service

No existing IGOSS applications require a full seven-layered OSI Connectionless service; however, a number of non-IGOSS protocols widely available in industry currently use similar protocols and can efficiently adapt to the use of OSI Upper Layer Connectionless protocols as an OSI transition mechanism. The OSI Upper Layer Connectionless protocols support one-way, unacknowledged information exchange without the reliability or overhead of the connection-oriented protocols. The Connectionless Upper Layer protocols include Connectionless ACSE [ISO 56], Connectionless Presentation [ISO 57], and Connectionless Session [ISO 58] and they operate over the Connectionless mode Transport protocol.

These protocols may be specified by procurement authorities in addition to the mandated protocols listed in Sections 3.2 and 3.3 in order to support user applications. Connectionless ACSE shall be implemented as specified in Part 5, clause 5.5 of the Workshop Agreements. The Connectionless Presentation protocol shall be implemented as specified in Part 5, clause 8.7 of the Workshop Agreements. The Connectionless Session protocol shall be implemented as specified in Part 5, clause 9.4 of the Workshop Agreements.

Figure 3.2.12 shows the protocols that provide the OSI Upper Layer Connectionless Application Subprofile.

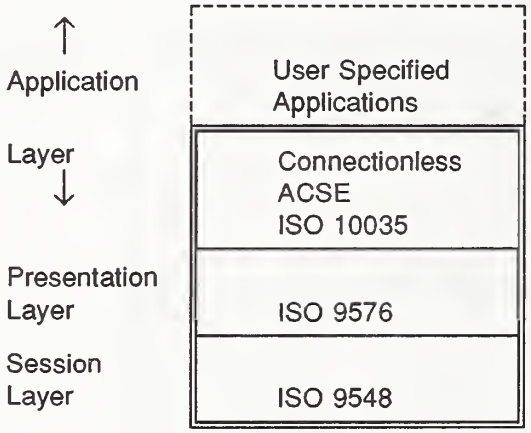


Figure 3.2.12. Connectionless Upper Layers Subprofile.

3.2.12.1 Requirements for Combination with Specific Upper Layer Subprofiles

This application subprofile requires the use of the Connectionless Transport Service. As such it must be combined with the CLTS-CLNS lower layer subprofile to define a complete procurement.

3.2.13 Minimal OSI (mOSI) Upper Layers Service

Many connection oriented OSI application protocols and virtually all non-OSI application protocols only require a minimal subset of OSI upper layer functionality, i.e., associate/release (connect/disconnect) and send/receive. Minimal OSI is a conformant subset of the ACSE protocol [ISO 23], Presentation Layer protocol [ISO 21] and Session Layer protocol [ISO 15] that provides basic communication services for application protocols that do not need a full OSI upper layer stack. Minimal OSI stack implementations will interoperate with full stack upper layer implementations where only basic communications services are required.

A mOSI compliant stack can be used to support a wide range of connection oriented network applications, for example,

a) the majority of OSI applications which do not use the more complex OSI upper-layer functions (e.g., resynchronization), e.g., all the ROSE based protocols (unless they map to RTSE),

b) virtually all of the byte stream connection oriented application protocols such as the X-windows protocol (see sec. 3.2.10), and

c) most of the so-called "legacy," non-OSI, application protocols.

The Minimal OSI ISP [ISO 112] is an ISP for the upper three layers of OSI which provides the required basic subset of the OSI services. The IGOSS Minimal OSI subprofile (**IGOSS1 mOSI**) is defined in Part 5, Annex D of the Workshop Agreements. Appendix 5 of this document specifies an Application Programming Interface that can be used to facilitate access to Minimal OSI services.

Figure 3.2.13 depicts the mOSI upper layers subprofile.

When used with non-OSI application protocols which were not designed to use the OSI presentation context negotiation facilities, mOSI provides dummy parameters to effect a byte stream context so that the migration of the non-OSI application protocol to use mOSI requires a minimum of change to the application (note: the application's addressing must always be changed).

See Section 8 of Appendix 3 for additional information.

3.3 OSI ACCOMMODATION FOR EXCHANGE FORMATS

Exchange formats are standard based representations of information entities (e.g., documents, graphics) for purposes of exchange. Exchange formats are referenced in the IGOSS because the information that they describe can be transported by the OSI FTAM and MHS protocols either as the content of a file or as the body part of a message. The exchange formats listed in this section are examples of candidates to use FTAM and MHS for this purpose. Exchange formats can also be transported by other mechanisms which are outside the scope of the IGOSS.

The Office Document Architecture (ODA) exchange format [ISO 36-42, CCITT 17-24] specifies rules for describing the logical and layout structures of documents as well as rules for specifying character, raster, and geometric content of documents, thus, providing for the interchange of complex documents. The interchanged documents may be in formatted form (i.e., for presentation such as printing, displaying), in processable form (i.e., for further processing such as editing) or in formatted processable form (i.e., for both presentation and further processing).

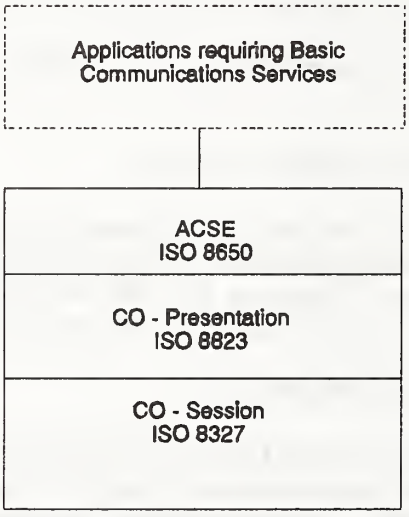


Figure 3.2.13. Minimal OSI (mOSI) Upper Layers Subprofile.

The Computer Graphics Metafile (CGM) exchange format [ISO 109] facilitates the transfer of picture description information between different graphical software systems, different graphical devices and different computer graphics installations. CGM specifies a file format suitable for the description, storage and communication of picture description information in a device-independent manner.

The Standard Generalized Markup Language (SGML) exchange format [NIST 12] provides a coherent and unambiguous syntax for describing whatever a user chooses to identify within a document. It is a metalanguage for describing the logical and content structure of a document in a machine processable syntax.

The Initial Graphic Exchange Specification (IGES) exchange format [ANSI 6] provides a neutral mechanism for the interchange of (CAD-CAM) information. IGES does not cover the complete life-cycle of manufactured products. It addresses only the specification of products, not the manufacturing process relationships.

The standard for the Exchange of Product Model Data (STEP) [ISO 105] is a family of related parts, including an information modeling language (EXPRESS), which provides a basis for the exchange of any data needed to support any stage in the life cycle of an engineered product.

For OSI product procurement purposes, the availability of a format exchange capability within MHS and FTAM is essential to the productivity and usefulness of the OSI products. IGOSS compliant products shall provide the means for binary file exchange with a user defined format identification. The identification tag will provide the means of identification for purposes of automated processing. MHS Bodypart 15 provides for the transport of user defined formatted messages including industry standard formats such as documents and spreadsheets.

In addition, Part 8, Annex D.5 of the Workshop Agreements contains information on how to identify and transport the ODA body part in an MHS message. Information on how to identify and transport additional exchange formats as the body part of a message or the content of a file will be added to future versions of the Workshop Agreements.

3.4 LOWER LAYER SUBPROFILES

This section defines the IGOSS lower layer subprofiles for services and protocols in the Transport and Network layers. The acquisition authority must select at least one subprofile from among this set for the provision of OSI lower layer services.

In selecting lower layer subprofiles, the acquisition authority must determine the OSI communication role(s) a system must support. For the provision of end system services IGOSS mandates support of the COTS-CLNS subprofile and provides for the selection of additional, optional CLTS-CLNS and COTS(X)-CONS lower layer services. For the support of intermediate system services IGOSS mandates support of the CLNS-Relay subprofile.

The complete set of requirements of Transport and Network Layer protocols are a combination of the selected lower layer subprofiles, service interfaces, and performance requirements. Particular attention should be paid to the additional functional and interface requirements upon Network Layer protocols (e.g., CLNP, ES-IS, IS-IS, X.25) dictated by the subnetwork subprofiles with which they are combined.

3.4.1 Transport Services

The selection of end system Transport services is dictated by the requirements of the applications selected for a given system. Most IGOSS application subprofiles (see fig. 2.1) require the use of the Connection Oriented Transport Service (COTS). The IGOSS also provides the option of supporting a Connectionless Mode Transport Service (CLTS). Although no specific IGOSS applications require support of the CLTS, IGOSS does provide, as an option, a generic Connectionless Upper Layers (CLUL) application subprofile.

The selection of protocol mechanisms to provide a chosen Transport service is dictated by the Network services over which the Transport protocol will operate. The end system lower layer subprofiles provide the appropriate combinations of Transport protocol mechanisms (classes) for each IGOSS Network service.

3.4.2 Network Services

The selection of network services is dictated by the collection of subnetwork technologies that comprise a system's communication environment. Achieving OSI is best accomplished by using a single protocol to perform the functions of end-to-end data communication within the Network Layer. To insure Network Layer interoperability IGOSS mandates the provision of the Connectionless Mode Network Service (CLNS) through the support of the Connectionless Mode Network Protocol (CLNP).

The IGOSS1 COTS-CLNS and CLNS-Relay subprofiles define the mandated CLNS for end systems and intermediate systems respectively. Several aspects about the effective procurement and deployment of CLNS inter-networks are not captured in the subprofile protocol requirements. In particular the design and development of an effective CLNS routing and addressing plan is fundamental to the acquisition and deployment of these profiles in real networks.

The acquisition authorities should consider the basic issues of CLNS routing and addressing in the development of such plans. The issues are described in the following sources:

1. IGOSS Section 4.
2. Workshop Agreements, Part 3, clauses 7 and 8.
3. RFC-1237 Guidelines for OSI NSAP Allocation in the Internet [MISC 4].
4. The IS-IS intra-domain routing protocol [ISO 49].
5. The IDRP Inter-domain Routing Protocol [ISO 102].

Additional CLNS requirements for individual systems (e.g., possibly based upon the logical or physical topology of a network, or the organization of real equipment in to routing subdomains) may be specified as the result of developing a specific routing and addressing plan. The acquisition authority is responsible for specification of any requirements that are in addition to those dictated in the IGOSS CLNS subprofiles.

The IGOSS also provides the additional option of supporting the Connection-Oriented Network Service (CONS) for end systems that are directly attached to X.25 packet-switching services (e.g., X.25 WAN, ISDN packet handler). Use of the CONS can, under certain circumstances, avoid the overhead associated with CLNP and might permit interoperation with end systems that do not comply with IGOSS (i.e., do not support the mandated CLNP). In addition, certain deployments of applications (e.g., MHS systems directly attached to CCITT public messaging services) require the support of this Network Layer service.

3.4.3 Subnetwork Services

The IGOSS provides a wide variety of standard subnetworking technologies (e.g., LAN, WAN, ISDN, Frame Relay, Point-to-Point leased lines) through the definition of Subnetwork Subprofiles. These technologies exhibit physical, functional, performance, and cost differences that render some subprofiles

more appropriate than others for particular deployments. The acquisition authority must specify one, or more, subprofile, for each real subnetwork interface of a system.

3.4.4 Support of OSI Management Information

The acquisition authority may optionally require the support of standardized management information for the resources of the Network and Transport layers. In particular, when management information support is selected an implementation of one of these subprofiles shall:

1. Conform, as a managed system, to Elements of Management Information Related to OSI Transport Layer Standards [ISO 84].

2. Conform, as a managed system, to Elements of Management Information Related to OSI Network Layer Standards [ISO 82].

3. Conform, as a managed system, to the managed object definitions contained in specific protocol standards (e.g., IS-IS [ISO 83], IDRP [ISO 102]).

In each case the system shall conform to the protocol/service specific requirements for management information that correspond to the communication resources selected in the subprofile. Selection of this minimal required management information can be indicated by appending the notation "/M" to any lower layer subprofile procurement category. For example the procurement category "COTS-CLNS/M" describes the mandatory end system lower layer subprofile that includes support for the elements of OSI management information specified above.

Acquisition authorities may optionally require additional management information for other resources of these subprofiles (e.g., data link or subnetwork resources) and/or additional "management views" of the resources of the Transport and Network layers. Any such additional specification should follow the requirements and guidance defined in the Management Information section of the Network Management application subprofile.

All supported management information shall be accessible to the communication services and systems management functions specified in the IGOSS1 Network-Management subprofile for this system.

3.4.5 COTS-CLNS Subprofile

Support of the COTS-CLNS subprofile depicted in Figure 3.4.5 is mandated for interoperability among all IGOSS systems and is the required means of providing a reliable end-to-end data communication.

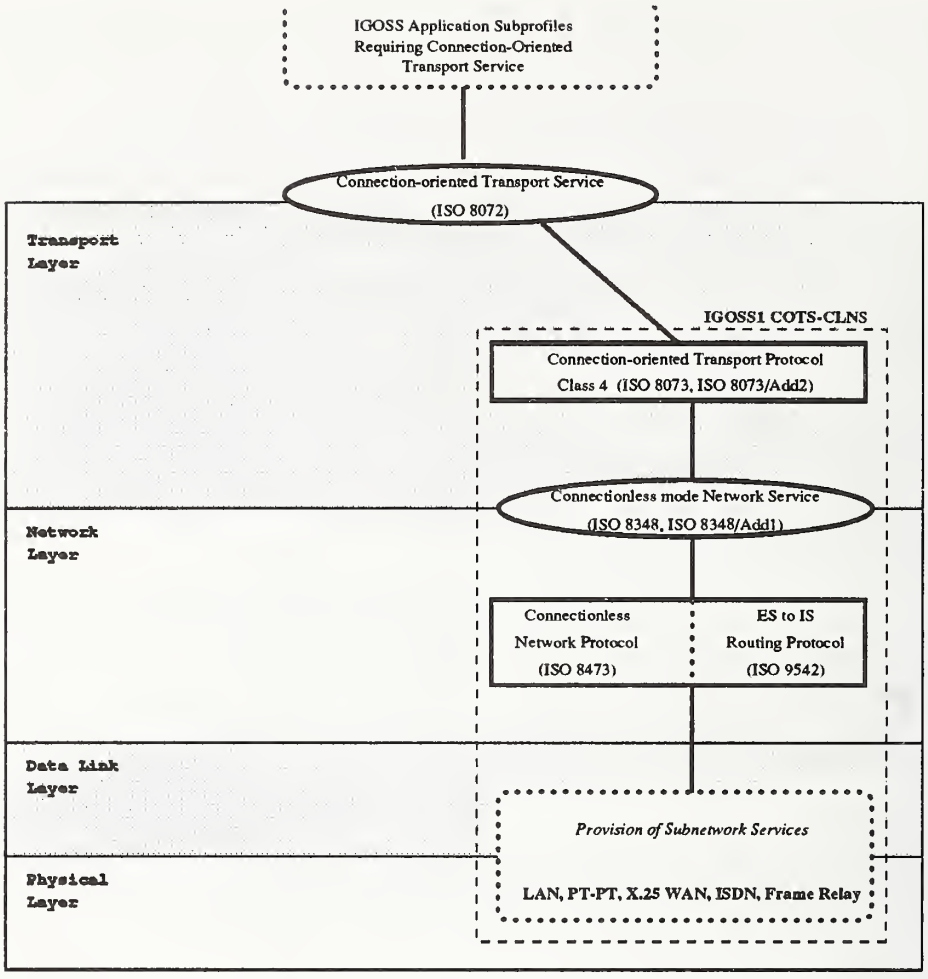


Figure 3.4.5. COTS-CLNS Subprofile.

The mandatory support of a single transport protocol class (class 4) and a single means of subnetwork inter-connection (use of the CLNP) assures interoperable data transfer between computer systems for a variety of upper layer applications across a variety of subnetwork technologies.

The acquisition authority shall select support of the COTS-CLNS profile for all systems that will operate as OSI end systems. Other IGOSS end system lower layer subprofiles may be selected in addition to this subprofile. In particular, the acquisition authority may specify support of the COTS(X)-CONS, and/or CLTS-CLNS end system lower layer subprofiles in addition to COTS-CLNS.

For the purposes of identification (e.g., in directory "protocol information" attributes) the COTS-CLNS subprofile is assigned the object identifier:

{ISO/CCITT (2), DCC (840), GOV (101), IGOSS(1), IGOSS1 COTS-CLNS (1)}

3.4.5.1 Provision of the Connection-Oriented Transport Service

This subprofile requires the provision of the Connection-Oriented Transport Service through the support and use of Transport Protocol Class 4 [NIST 1; ISO 12,13].

3.4.5.1.1 Transport Protocol Class 4

Transport Protocol Class 4 shall be provided according to Part 4, clause 5.1 of the Workshop Agreements, with the following modifications and additions:

1. Replace item (f) of the Workshop Agreements Part 4, clause 5.1.2.1 with the following:

   It is recommended that implementations not send user data in the Connect Request (CR) or Connect Confirm (CC) TPDU. Any user data received in a CR or CC TPDU will be made available to the Transport Service user.

2. Replace item (g) of the Workshop Agreements Part 4, clause 5.1.2.1 with the following:

   It is recommended that implementations not send user data in the DR TPDU. Any user data received in a DR TPDU will be made available to the Transport Service user.

3. Add, as an addition item of the Workshop Agreements Part 4, clause 5.1.2.1, the following:

   Transport expedited shall be provided as an optional service for the Transport Service user.

3.4.5.2 Provision of the Connectionless Mode Network Service

This subprofile requires the provision of the CLNS through the support and use of the Connectionless Network Protocol (CLNP) [NIST 1; ISO 4,7] and End System to Intermediate System (ES-IS) Routing Protocol [ISO 44].

3.4.5.2.1 Connectionless Network Protocol (CLNP)

The CLNP shall be provided according to the Workshop Agreements Part 3, clause 5.1 with the following modifications and additions:

1. Add to item (a) of Part 3, clause 5.1 Mandatory Functions, the following:

   A System must provide a configuration mechanism to control the value to be assigned to the Lifetime parameter for PDUs which it originates.

2. Replace Part 3, clause 5.1.3 Optional Functions of ISO 8473 item (g) with:

   (g) All systems shall support the echo function as specified in ISO 8473/DAM6. All systems shall provide mechanisms through which the Echo request function may be invoked.

3.4.5.2.2 End System to Intermediate System Routing Protocol (ES-IS)

The ES-IS protocol shall be provided according to the Workshop Agreements part 3 clause 8.1.

3.4.5.2.3 Requirements for Combination with Specific Subnetwork Subprofiles

The following define additional requirements upon the provision of the CLNS protocols appropriate for specific subnetwork subprofiles. If the acquisition authority chooses to combine this subprofile with subnetwork technologies not included within this specification, the authority must provide proper specification of such interface requirements.

3.4.5.2.3.1 LANs

Part 3 clause 5.2 of the Workshop Agreements shall apply.

3.4.5.2.3.2 X.25 WAN

Part 3 clause 5.3 of the Workshop Agreements shall apply.

3.4.5.2.3.3 ISDN

Part 3 clause 5.4 of the Workshop Agreements shall apply.

3.4.5.2.3.4 Frame Relay

When providing the CLNS over PVCs, the frame relay subnetwork shall be logically treated as a collection of point-to-point links. The CLNS routing functions appropriate for operation on point-to-point links shall be operated.

The support of CLNS protocols over switched virtual circuit (SVC) frame relay services is for future study.

3.4.5.2.3.5 Pt-Pt

Part 3 clause 5.5 of the Workshop Agreements shall apply.

3.4.6 CLNS-Relay (X) Subprofile

The CLNS-Relay (x) subprofile depicted in Figure 3.4.6 is mandated for all systems that will operate as OSI intermediate systems. (Section 3.4.6.1.3 contains the values of the (x) variant) Connectionless inter-networking, through the use of the CLNP, is the required means of providing OSI Network Layer relaying regardless of the underlying subnetwork technologies. Note, however, that the inter-connection of distinct subnetworks to form the appearance of a single logical subnetwork may be performed by any technically appropriate means (e.g., MAC bridges, X.75 gateways).

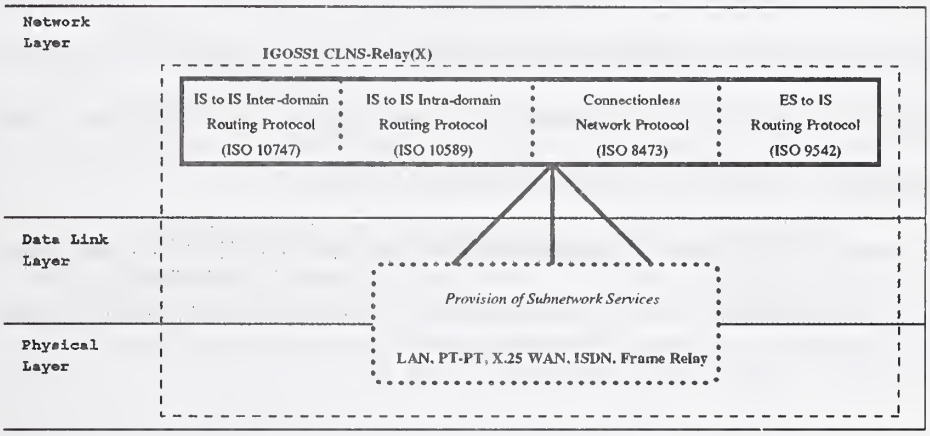


Figure 3.4.6. CLNS-Relay (X) Subprofile.

The mandatory support of a single means of subnetwork inter-connection (use of the CLNP) assures interoperable data transfer between computer systems for a variety of upper layer applications across a variety of subnetwork technologies. The CLNS-Relay subprofile requires the support of the ES-IS and IS-IS routing protocols for the dynamic exchange of CLNS routing and configuration information.

For the purposes of identification (e.g., in directory "protocol information" attributes) the COTS-CLNS subprofile is assigned the object identifier:

{ISO/CCITT (2), DCC (840), GOV (101), IGOSS(1), IGOSS1 COTS-CLNS (1)}

3.4.6.1 Provision of the Connectionless Mode Network Service

This subprofile requires the support of the CLNS through the provision and use of the Connectionless Network Protocol (CLNP) [NIST 1; ISO 4,7] End System to Intermediate System (ES-IS) Routing Protocol [ISO 49], and Intermediate System to Intermediate System Intra-domain Routing Protocol (IS-IS) [ISO 83]. The provision of the Intermediate System to Intermediate System Interdomain Routing Protocol IDRP) [ISO 102] may be selected as an option.

3.4.6.1.1 Connectionless Network Protocol (CLNP)

The CLNP shall be provided according to the Workshop agreements Part 3 clause 5.1 with the following modifications and additions:

1. Add to item (a) of part 3 clause 5.1 Mandatory Functions, the following:

   A System must provide a configuration mechanism to control the value to be assigned to the Lifetime parameter for PDUs which it originates.

2. Replace Part 3, clause 5.1.3 Optional Functions of ISO 8473 item (g) with:

   (g) All system shall support the echo function as specified in ISO 8473/DAM6. All systems shall provide mechanisms through which the Echo request function may be invoked.

3.4.6.1.2 End System to Intermediate System Routing Protocol (ES-IS)

The ES-IS protocol shall be provided according to the Workshop Agreements Part 3 clause 8.1.

3.4.6.1.3 Intermediate System to Intermediate System Routing

This subprofile requires the support of dynamic intermediate system to intermediate system routing protocols for the exchange of CLNS routing and configuration information. The routing protocols supported and the required capabilities of those protocols are a function of the role that an IS must be capable of operating in. The acquisition authority must specify an IS's basic dynamic routing capabilities as one of:

(**X=L1IS**) - Level 1 Intra-domain IS. The intermediate system shall support Level 1 IS-IS capabilities.

(**X=L2IS**) - Level 2 Intra-domain IS. The intermediate system shall support Level 2 IS-IS capabilities in addition to the capabilities of a L1IS. A L2IS system supports the capability of configuring static inter-domain routing information.

(**X=BIS**) - Border Inter-domain IS. The intermediate system shall support IDRP in addition to the capabilities of L2IS.

Note that the use of extensions to the IS-IS and/or IDRP protocols to provide "integrated routing" support for additional protocol suites (e.g., RFC-1195: Use of OSI IS-IS for Routing in TCP/IP and Multi-Protocol Environments) is not precluded by this profile.

While outside the scope of IGOSS, acquisition authorities should evaluate the requirements for such extensions in the context of an overall multi-protocol routing strategy. This analysis may result in the selection of additional optional IS-IS capabilities needed to support operation for protocols other than CLNP.

The following sections state the protocol specific requirements.

3.4.6.1.3.1 Intermediate System to Intermediate System Intra-domain Routing Protocol (IS-IS)

The IS-IS protocol shall be provided (X=L1IS, L2IS, or BIS) according to the Workshop Agreements Part 3 clause 8.3.2.

Add, as an additional item of the Workshop Agreements Part 3, clause 8.3.2, the following:

(c) When operating on IEEE 802.5 (i.e., token ring) LANs the group addresses specified in [ISO 83] clause 8.4.8 table 9 shall be used.

This subprofile places the following requirements on the provision of the IS-IS protocol:

1. Authentication based upon passwords shall be supported.

2. For L2ISs, reachable address prefixes shall be supported. Reachable address prefixes shall be capable of supporting all (i.e., explicit, IDI extraction and DSP extraction) next hop mapping types.

The acquisition authority shall specify any requirements for IS-IS capabilities that are optional in the base standard (e.g., support of non-default routing metrics, support of equal cost path splitting).

3.4.6.1.4 Intermediate System to Intermediate System Inter-domain Routing Protocol (IDRP)

If selected (X=BIS), the IDRP protocol shall be provided according to the Workshop Agreements Part 3, clause 8.4.2. The acquisition authority shall select an implementation subset as defined in the Workshop Agreements.

3.4.6.1.5 Requirements for Combination with Specific Subnetwork Subprofiles

The following define additional requirements upon the provision of the CLNS protocols appropriate for specific subnetwork subprofiles. If the acquisition authority chooses to combine this subprofile with subnetwork technologies not included within this specification, the authority must provide proper specification of such interface requirements.

3.4.6.1.5.1 LANs

Part 3 clause 5.2 of the Workshop Agreements shall apply.

3.4.6.1.5.2 X.25 WAN

Part 3 clause 5.3 of the Workshop Agreements shall apply.

3.4.6.1.5.3 ISDN

Part 3 clause 5.4 of the Workshop Agreements shall apply.

3.4.6.1.5.4 Frame Relay

When providing the CLNS over PVCs, the frame relay subnetwork shall be logically treated as a collection of point-to-point links. The routing functions appropriate for operation on point-to-point links shall be operated.

The support of CLNS protocols over switched virtual circuit (SVC) frame relay services is for future study.

3.4.6.1.5.5 Pt-Pt

Part 3 clause 5.5 of the Workshop agreements shall apply.

3.4.7 CLTS-CLNS Subprofile

The CLTS-CLNS subprofile depicted in Figure 3.4.7 is an optional end system lower layer subprofile for the provision of connectionless transport services.

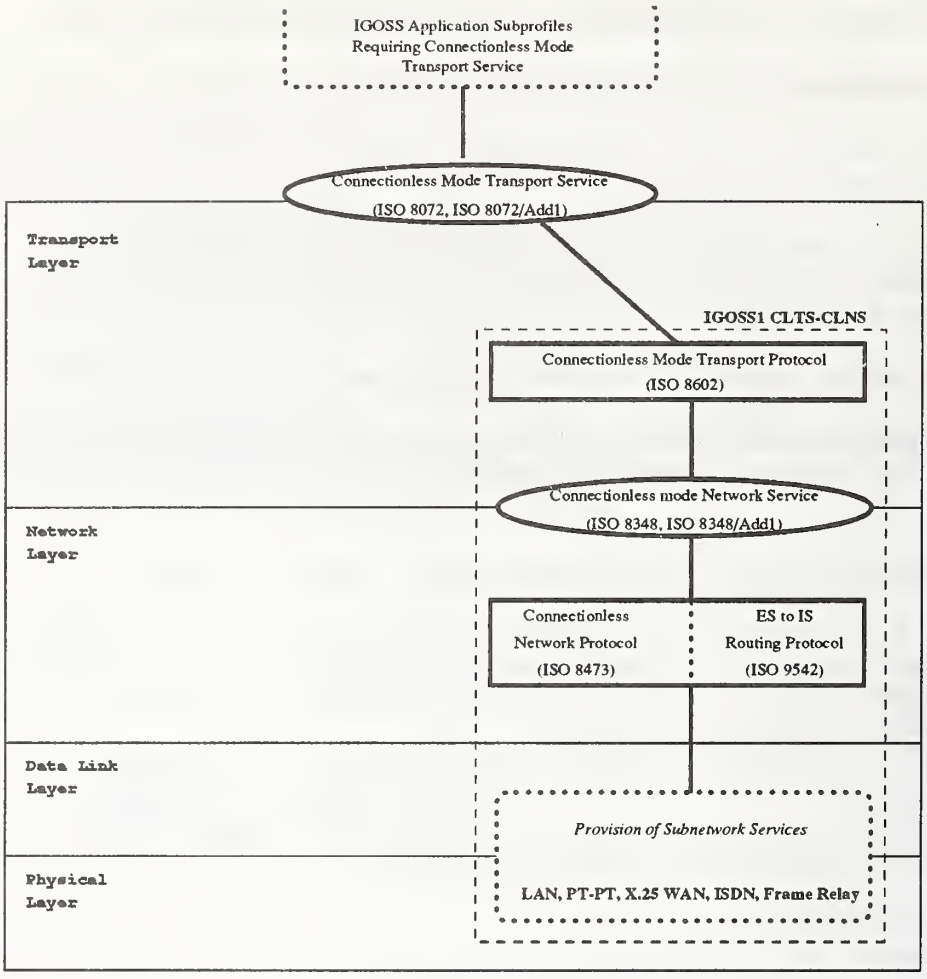


Figure 3.4.7. CLTS-CLNS Subprofile.

If required, the acquisition authority shall select support of the CLTS-CLNS subprofile in addition to the mandated COTS-CLNS subprofile.

For the purposes of identification (e.g., in directory "protocol information" attributes) the CLTS-CLNS subprofile is assigned the object identifier:

{ISO/CCITT (2), DCC (840), GOV (101), IGOSS(1), IGOSS1 CLTS-CLNS (3)}

3.4.7.1 Provision of the Connectionless Mode Transport Service

This subprofile requires the provision of the Connectionless Mode Transport Service through the support and use of the Connectionless Transport Protocol (CLTP) [NIST 1; ISO 47].

3.4.7.1.1 Connectionless Transport Protocol

The Connectionless Transport Protocol (CLTP) [NIST 1; ISO 47] shall be provided according to Part 4 clause 6.2 of the Workshop Agreements.

3.4.7.2 Provision of the Connectionless Mode Network Service

This subprofile requires the provision of the CLNS through the support and use of the Connectionless Network Protocol (CLNP) [NIST 1; ISO 4,7] and End System to Intermediate System (ES-IS) Routing Protocol [ISO 44].

The detailed CLNS requirements are specified in section 3.4.5.2 of the IGOSS.

3.4.7.2.1 Requirements for Combination with Specific Subnetwork Subprofiles

The requirements are specified in section 3.4.5.2.3 of the IGOSS.

3.4.8 COTS(X)-CONS Subprofile

The COTS(X)-CONS subprofile depicted in Figure 3.4.8 is an optional end system lower layer subprofile for the provision of Connection Oriented Transport Services (COTS) over the Connection Oriented Network Service (CONS). The acquisition authority must select the desired Transport Protocol class combinations (e.g., X=0, 0/2, 0/2/4) and specify whether the CONS ES-IS routing protocol is to be supported.

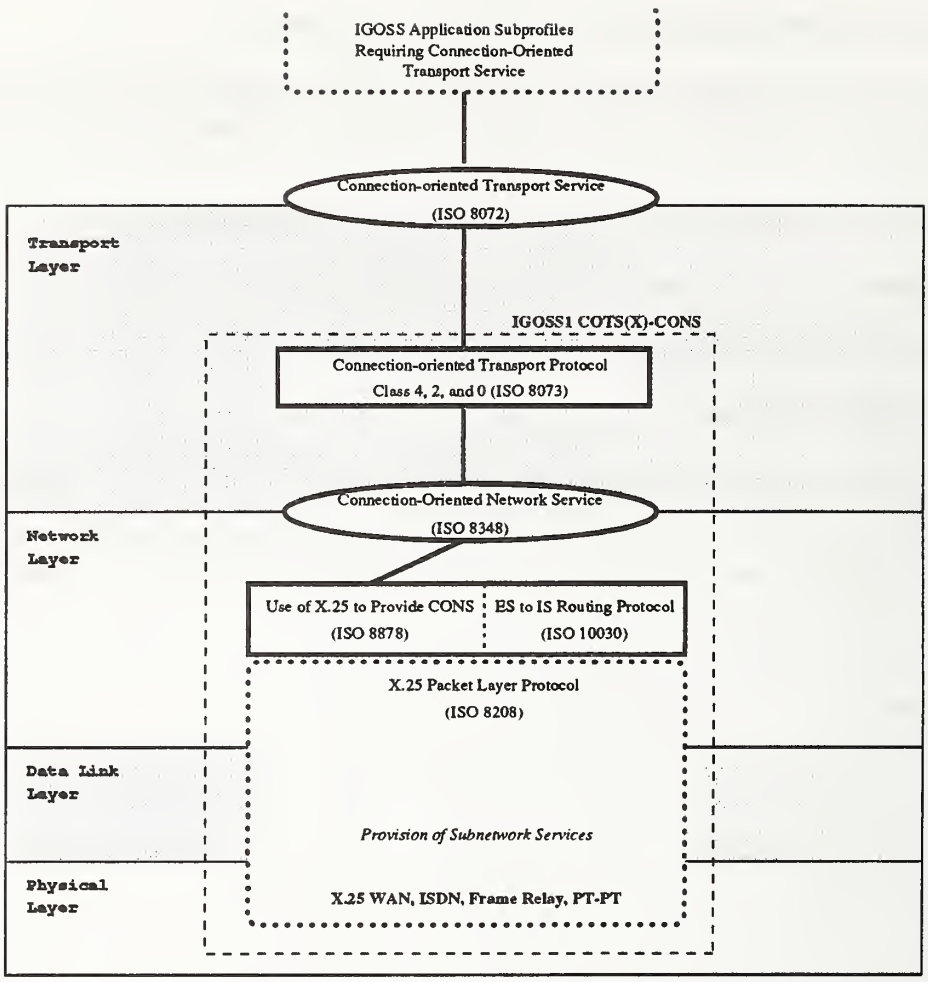


Figure 3.4.8. COTS(X)-CONS Subprofile.

The COTS-CONS subprofile may be selected for end systems that are directly attached to X.25 packet-switching services (e.g., X.25 WAN, ISDN packet handler). Use of the CONS can, under certain circumstances, avoid the overhead associated with CLNP and might permit interoperation with end systems that do not comply with IGOSS (i.e., do not support the mandated CLNP). In addition, certain deployments of applications (e.g., MHS systems directly attached to CCITT public messaging services) require the support of this subprofile.

If required, the acquisition authority shall select support of the COTS-CONS subprofile in addition to the mandated COTS-CLNS profile.

For the purposes of identification (e.g., in directory "protocol information" attributes) the COTS-CONS subprofile is assigned the object identifier:

{ISO/CCITT (2), DCC (840), GOV (101), IGOSS(1), IGOSS1 COTS-CONS (4)}

3.4.8.1 Provision of the Connection-Oriented Transport Service

This subprofile requires the provision of the COTS through the support and use of the Transport Protocol [NIST 1; ISO 12,13]. The acquisition authority must select the Transport protocol class combinations appropriate for specific applications of this subprofile. The allowed class combinations are: (X=0), (X=0,2), and (X=0,2,4).

In operating the Transport Protocol over ISO 8202/X.25, the rules for Transport Protocol identification stated in Part 4 clause 7 of the Workshop Agreements shall apply.

3.4.8.1.1 Transport Protocol Class 4

If selected by the acquisition authority, Transport Protocol Class 4 shall be provided according to Section 3.4.5.1.1 of the IGOSS.

3.4.8.1.2 Transport Protocol Class 2

If selected by the acquisition authority, Transport Protocol Class 2 shall be provided according to Part 4 clause 5.3 of the Workshop Agreements.

3.4.8.1.3 Transport Protocol Class 0

If selected by the acquisition authority, Transport Protocol Class 0 shall be provided according to Part 4 clause 5.2 of the Workshop Agreements.

3.4.8.2 Provision of the Connection-Oriented Network Service

This subprofile requires the provision of the CONS through the support and use of the ISO 8208 X.25 Packet Layer Protocol.

3.4.8.2.1 X.25 Packet Layer Protocol

The X.25 Packet Layer Protocol (PLP) [ISO 2] shall be provided according to part 3 clause 6.1.1 of the Workshop agreements. The X.25 PLP shall provide DTE to DCE capabilites. If desired, the acqusition authority may additionally require the support of DTE to DTE capabilities in the provision of the X.25 PLP.

3.4.8.2.2 CONS End System to Intermediate System Routing Protocol (CONS ES-IS)

The acquisition authority may optionally require the support of the CONS ES-IS protocol in environments in which ISO-10030 Subnetwork Address Resolution Entities (SNAREs) are to operate.

If selected, the CONS ES-IS protocol [ISO 100] shall be provided according to the Workshop Agreements Part 3 clause 8.2.

The acquisition authority shall indicate whether the CONS ES-IS protocol shall support End System functions, SNARE functions, or both. In each case, both the Configuration Subset and the Route Redirection subset shall be provided.

3.4.8.2.3 Requirements for Specific Subnetwork Subprofiles

The following define additional requirements upon the provision of the CONS appropriate for specific subnetwork subprofiles. If the acquisition authority chooses to combine this subprofile with subnetwork technologies not included within this specification, the authority must provide proper specification of such interface requirements.

3.4.8.2.3.1 X.25 WAN

There are no additional requirements.

3.4.8.2.3.2 ISDN

When providing CONS in an ISDN, the considerations for control of B and D channels shall be provided by ISO 9574 [ISO 45] and implemented according to Part 3 clause 6.1.4 of the Workshop Agreements.

3.4.8.2.3.3 Pt-Pt

The acquisition authority should specifiy the support of DTE-DTE facilities in the X.25 PLP.

3.4.9 Subnetwork Subprofiles

This section defines the IGOSS subnetwork subprofiles. The acquisition authority should select one subprofile from among this set for each real subnetwork interface of a system. These technologies exhibit physical, functional, performance, and cost differences that render some subprofiles more appropriate than others for particular uses.

In circumstances in which specific deployment requirements can not be met by any of the technologies provided by the IGOSS1 subnetwork subprofiles, other technologies may be used. In such cases the acquisition authority must provide a proper subnetwork subprofile specification, including conformance requirements, so as to ensure the procurement of an effective product; that is, a product that is capable of supporting the selected IGOSS lower layer subprofiles and can interoperate with other IGOSS systems to be attached to the subnetwork.

3.4.9.1 LAN(X,Y) Subprofiles

Figure 3.4.9.1 depicts the IGOSS subprofile choices for LAN interfaces. The acquisition authority must select the basic LAN technology to be provided (X = CSMA/CD, FDDI, Token Ring, or Token Bus) and the specific Physical Media Dependent (PMD) characteristics (Y = 10Base2, MMF-PMD, etc.) for each LAN interface.

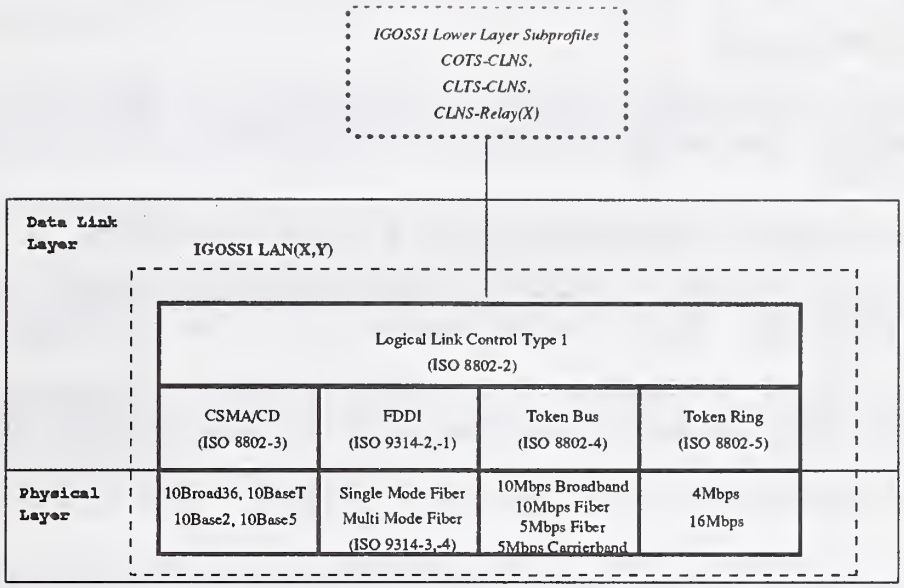


Figure 3.4.9.1. LAN Subnet Subprofile.

The interconnection of distinct LANs to form the appearance of a single logical subnetwork may be accomplished by any technically appropriate means, such as MAC bridges. In order to ensure interoperation of IGOSS LAN subprofiles, the acquisition authority is advised to cite appropriate standards (e.g., ISO 10038 [ISO 103]) in the specification of such interconnection devices.

There may be situations in which LAN interfaces are required to support non-standard physical media. While use of non-standard media is discouraged, such LAN interfaces are not excluded from IGOSS. In these situations, the acquisition authority must provide proper specification, including conformance requirements, of the PMD characteristics of the interface.

3.4.9.1.1 Logical Link Control Services

All IGOSS1 LAN(X,Y) subprofiles shall provide Logical Link Control services through the support and use of the Logical Link Control Type 1 procedures [NIST 1; ISO 28] as specified in Part 2 clause 5.1 of the Workshop Agreements. For each LAN interface the acquisition authority must select from the following standard LAN technologies.

3.4.9.1.2 CSMA/CD LANs

If selected, CSMA/CD LAN interfaces shall be provided as specified in [ISO 29] and Part 2 clause 5.2 of the Workshop agreements. The acquisition authority shall specify the PMD characteristics of the interface (Y = 10Broad36, 10BaseT, 10BaseF, 10Base2, or 10Base5).

3.4.9.1.3 FDDI LANs

If selected, FDDI LAN interfaces shall be provided as specified in [ISO-95-99] and Part 2, clause 5.5 of the Workshop Agreements. To define an effective FDDI procurement the acquisition authority must specify

the PMD characteristics and Station Management (SMT) requirements for the FDDI interface. The following sections note issues that must be addressed in making this selection.

3.4.9.1.3.1 FDDI PMD Variants

FDDI PMD standards for multimode (Y = MMF-PMD) and single mode (Y = SMF-PMD) are stable and interoperable products are available. When the MMF-PMD is selected, part 2 clause 5.5.3 of the Workshop Agreements shall apply.

Standards for several other PMD variants are now being developed. These include:

1. Low Cost Fiber PMD (Y = LCF-PMD), which will be interoperable with PMD, however when LCF-PMD is used in either port of a link, that link is limited to a distance of 500 m rather than 2 km.

2. Twisted Pair PMD (Y = TP-PMD), which will allow the use of either 150 Ohm shielded twisted pair or "category 5," unshielded, data grade, 100 Ohm twisted pair wire. Link distance is limited to 100 m.

3. SONET Physical Mapping (Y = SPM), which will allow FDDI links to be carried over SONET STS-3 channels.

At the present time there are several commercially available products which provide FDDI over shielded or unshielded twisted pair media. These may not conform to the final TP-PMD standard, and products from different vendors may not interoperate. Acquisition authorities that wish to procure products based upon these emerging standards must take care to ensure the procurement of effective products.

3.4.9.1.3.2 FDDI Station Management (SMT)

The evolution of FDDI SMT standards has recently stabilized. The ANSI X3T9 approved Version 7.2 of SMT [ANSI 12] is considered as a mature and stable candidate for adoption as the ISO SMT standard. As the ISO SMT standard [ISO 99] matures to incorporate a stable SMT specification, acquisition authorities should migrate to the use of the ISO standard as the primary reference specification. It should be noted that some functional profiles have adopted an interim specification based on version 6.2 of the ANSI SMT specification. Procurement authorities should specificly address requirements for SMT interoperation with other, non-IGOSS compliant, SMT implementations.

Each FDDI interface shall support the following aspects of station management as defined in Version 7.2 of SMT.

1. Physical Connection Management (PCM), which is required to initialize FDDI connections, that is the data link between two FDDI ports.

2. Configuration Management (CFM), which manages the internal configuration of an FDDI network node.

3. Ring Management (RMT), which controls the initialization of FDDI rings and resolves duplicate address problems which may occur.

4. Management Information Base (MIB), which defines the managed objects and attributes of FDDI.

5. Frame Based Management, which defines direct FDDI SMT to FDDI SMT management frames, that do not use layers above MAC.

Note that there is optional functionality inherent in PCM, CFM, RMT, and SMT that may eventually become the subject of additional implementation agreements as trends in user's requirements and vendor's support for station management mature.

Presently it is the acquisition authority's responsibility to evaluate, in the context of an overall strategy for LAN/system's management, any additional SMT requirements. Any such requirements should be reflected in the selection of which of these options are to be supported by individual FDDI interfaces.

3.4.9.1.4 Token Ring LANs

If selected, Token Ring interfaces shall be provided as specified in [ISO 31] and Part 2 clause 5.4 of the Workshop Agreements. The acquisition authority shall specify the PMD characteristics of the interface (Y=4Mbit, or 16Mbit).

All token ring interfaces shall support the use of Group MAC Addressing in accordance with ISO 8802-5. It is strongly recommended that Group addresses be used to support all OSI uses of multicast on token ring networks. In some deployment scenarios it may be necessary to use Functional Addressing in order to interoperate with existing installed systems that have limited, or no ability to support group addresses.

In general, for each token ring LAN, all ESs and ISs shall use exclusively either functional addresses or group addresses in the operation of a given OSI protocol (e.g., ES-IS, IS-IS). In instances where group addresses must be used to interoperate with existing deployed systems, acquisition authorities should be warned that the ability to interconnect such LANs with other IGOSS LANs through the use of MAC sublayer bridges will be greatly complicated.

Acquisition authorities should consult the appropriate lower layer subprofiles for specific restrictions and recommendations regarding these issues.

3.4.9.1.5 Token Bus LANs

If selected, Token Bus interfaces shall be provided as specified in [ISO 30] and part 2 clause 5.3 of the Workshop Agreements. The acquisition authority shall specify the PMD characteristics of the interface (Y = 10Mbps Broadband, 5Mbps Carrierband, 5Mbps Fiber or 10Mbps Fiber).

3.4.9.2 X25-WAN Subprofile

Figure 3.4.9.2 depicts the subprofile applicable to the use of X.25 to interface with Wide Area Network (WAN) packet-switching services. For subnetwork interfaces to ISDN X.25 packet-switching services, see the IGOSS1 ISDN-X25(X) subprofile in Section 3.4.9.3.1.

The elements of ISO 8208 applicable for use depend upon the OSI role in which the X.25 PLP (i.e., provision of the CONS, support of the CLNP) is used. This subprofile states the role independent of requirements for X.25 WAN interfaces. Additional role dependent requirements are specified in the IGOSS Lower Layer subprofiles.

The X25-WAN subprofile requires that:

1. The X.25 PLP [ISO 8] and LAPB shall be provided as specified in part 2 clause 6 of the Workshop Agreements.

2. This subprofile does not mandate any specific physical interface standard. The acquisition authority must specify the desired physical interface standards (protocol and connector) for each interface.

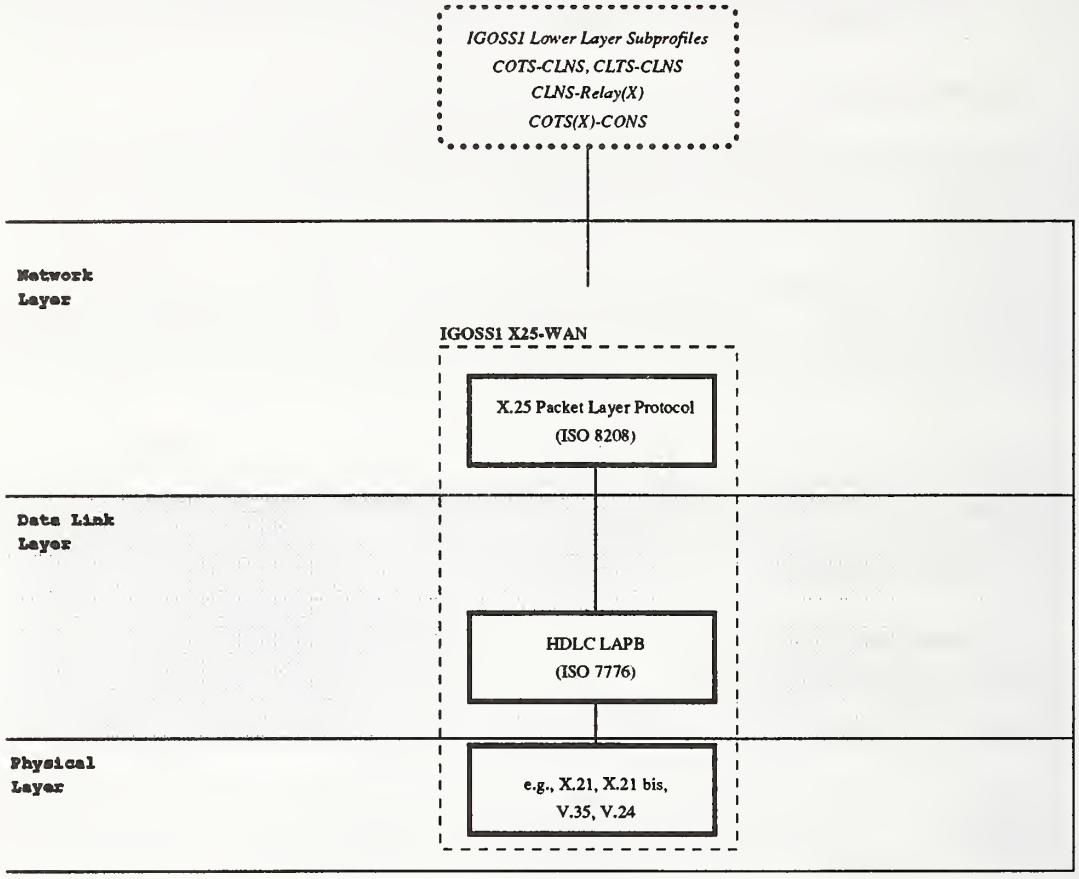


Figure 3.4.9.2. X25-WAN Subprofile.

3.4.9.3 ISDN Subprofiles

This set of subprofiles specify the scenarios in which ISDN interfaces can be used to provide subnetwork services to the IGOSS Lower Layers.

3.4.9.3.1 IGOSS1 ISDN-X25(X) Subprofiles

Figure 3.4.9.3.1 depicts the subprofiles applicable to the use of an ISDN to provide X.25 packet-switching services.

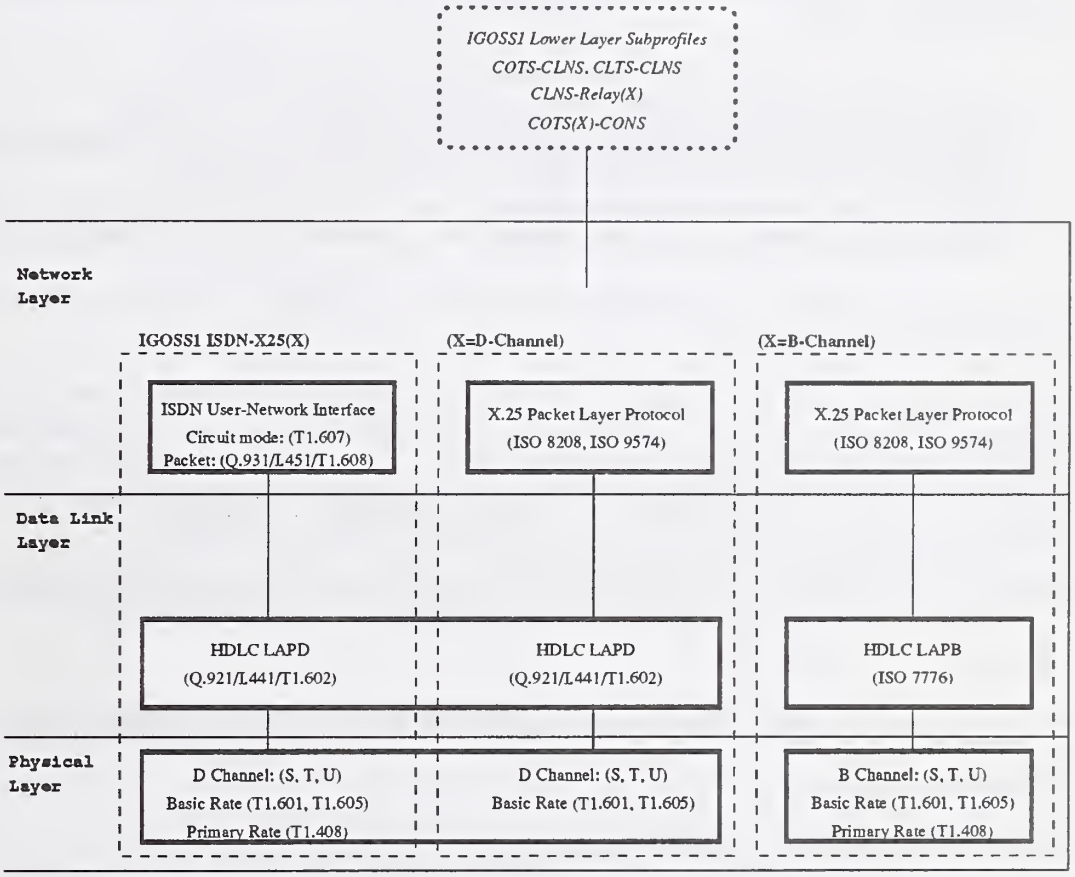


Figure 3.4.9.3.1. ISDN X.25(X) Subprofile.

Integrated services digital networks (ISDN) support X.25 packet-switching services on the D channel (X=D-Channel), sharing the channel with signaling data, and on the B channel (X=B-Channel). In either scenario, call control signalling shall be provided as specified in the Workshop Agreements part 2 clause 7.2.5.

For each ISDN interface the acquisition authority must specify the common call control signalling (ISDN-X25(X)) and one or both of the packet-switching capabilities.

ISDN provides the possibility of a Basic Rate Interface (BRI) (16 Kbps D-channel + 2 64 Kbps B-channels) or a Primary Rate Interface (PRI) (64 Kbps D-channel + 23 64 Kbps B- channels). The acquisition authority must specify whether BRI or PRI is required for each ISDN interface. The BRI service interface

might be available at the S, T, or U reference point. For ISDN physical layer access at the S, T, and U reference points, Part 2 clauses 7.2.1, 7.2.2 and 7.2.3 of the Workshop Agreements apply. The acquisition authority must specify the physical interface required for each BRI.

The X.25 PLP for use on ISDN B and D channels shall be provided as specified in Part 2 clause 7.2.7 of the Workshop Agreements.

3.4.9.3.1.1 B-Channel Operation

When operation of X.25 over a B-Channel is selected, ISDN B-channel services can be used by an IGOSS system in several ways:

1. circuit-switched access to a packet handler integral to an ISDN switch;
2. circuit-switched access to a packet handler separate from an ISDN switch;
3. circuit-switched access directly to another IGOSS end system, or IGOSS intermediate system;
4. dedicated circuit access to a packet handler integral to an ISDN switch;
5. dedicated circuit access to a packet handler separate from an ISDN switch, and
6. dedicated circuit access to another IGOSS end system or IGOSS intermediate system.

The acquisition authority must specify the B-channel access capabilities required for each ISDN interface with ISDN B-channel services.

(Note that at the present time switched access to the B channel is available from most ISDN vendors, but not in a standard fashion; thus, multi-vendor interoperability between terminal equipment and switching equipment is not widely available today. Work underway in the North American ISDN User Forum (NIUF) is expected to improve this situation in the future. As appropriate NIUF Agreements are developed, and related ISDN FIPS are issued by NIST, IGOSS will be updated accordingly.)

For data link layer access on a B channel, Part 2 clause 7.2.6 of the Workshop Agreements applies.

3.4.9.3.1.2 D-Channel Operation

For data link layer access on the D channel, Part 2 clause 7.2.4 of the Workshop Agreements applies.

3.4.9.4 PVC-Frame-Relay

Figure 3.4.9.4 depicts the subprofile for data transfer and local management status and control information between user equipment and frame relay permanent virtual circuit (PVC) network services. The protocols for the access and provision of frame relay data transfer services shall be provided according to part 2 clause 8 of the Workshop Agreements. Additional requirements for signalling when frame relay services are provided within the context of an ISDN are described in Section 3.4.9.3.

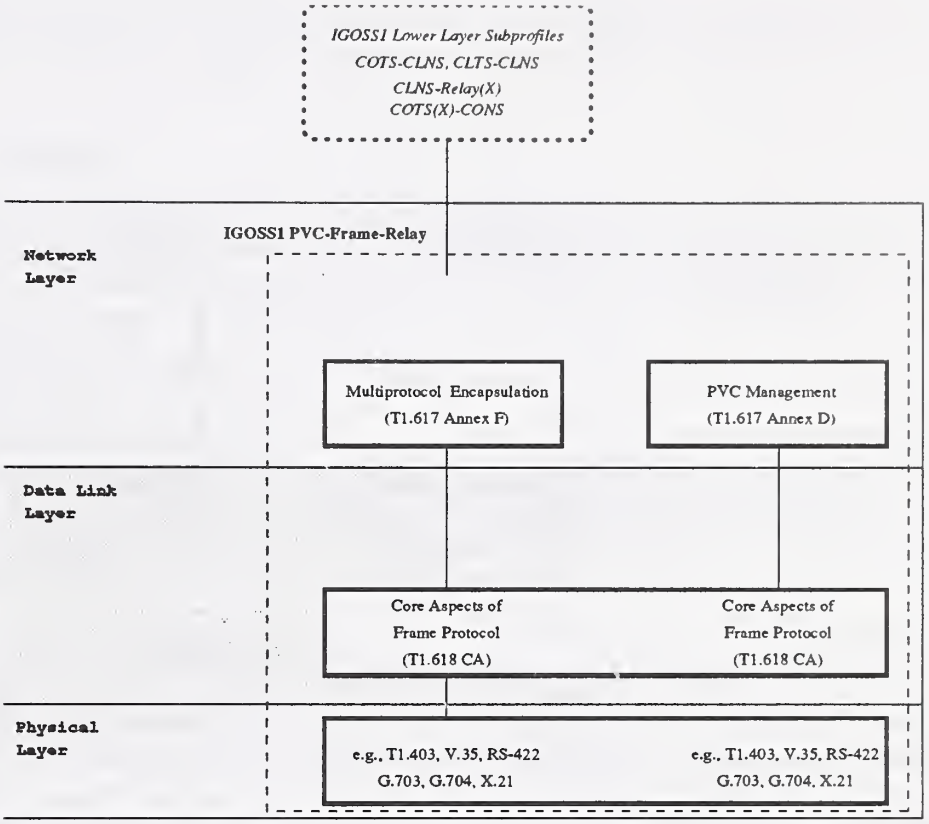


Figure 3.4.9.4. PVC-Frame Relay Subprofile.

The encapsulation scheme for the transmission of OSI network layer protocols on frame relay subnetworks is consistent with the procedures for protocol identification specified in part 3 clause 9 of the Workshop Agreements. The definition of the encapsulation scheme, including the support of other uses (e.g., bridging, non-OSI protocols) of frame relay services, shall be as specified in Annex F of [ANSI 9].

3.4.9.5 Point-to-Point(X) Subprofile

Figure 3.4.9.5 depicts the IGOSS subprofile choices for interfaces that support CLNS protocols directly over point-to-point data links. The acquisition authority must select the basic data link procedures (X = LAPB, or PPP) and the specific physical interface standards to be provided.

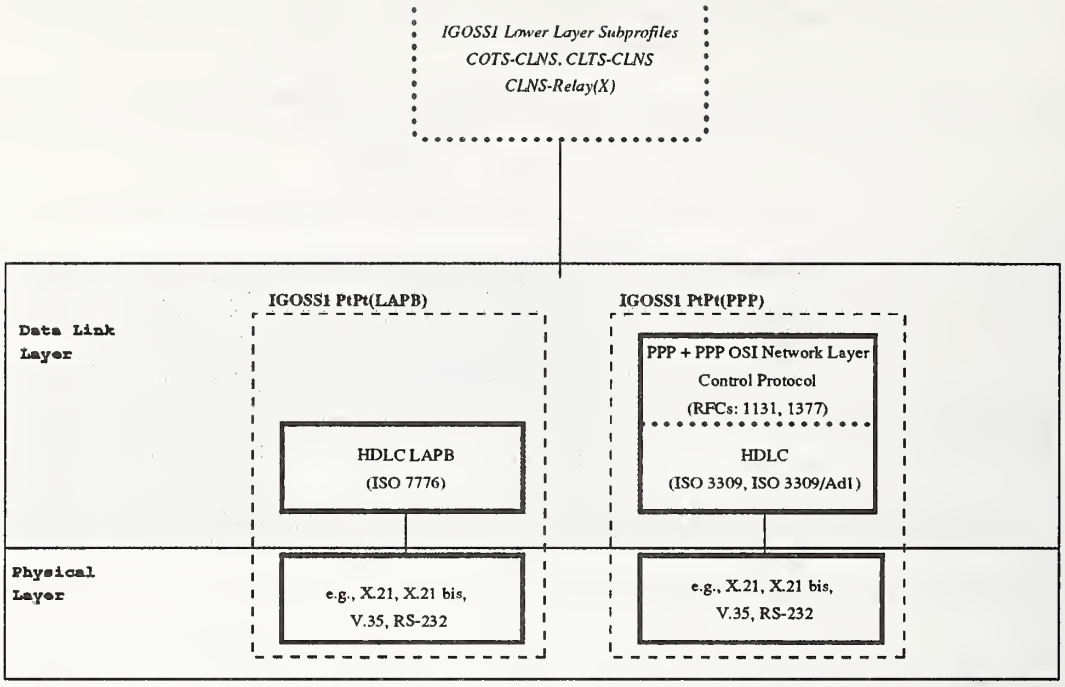


Figure 3.4.9.5. PtPt Subprofile.

These subprofiles do not mandate any specific physical interface standard. The acquisition authority must specify the desired physical interface standards (protocol and connector) for each interface.

3.4.9.5.1 LAPB Subprofile

The Point-to-Point(LAPB) subprofile requires that:

1. The LAPB protocol shall be provided as specified in clauses 4 and 5 of ISO 8880-3 [ISO 101], as appropriate.

2. The acquisition authority shall specify the desired physical interface standards (protocol and connector) for each interface.

3.4.9.5.2 PPP Subprofile

The Point-to-Point(PPP) subprofile requires that:

1. The Point-to-Point Protocol shall be provided as specified in RFC 1331 [MISC 3]. The PPP OSI Network Layer Control Protocol shall be provided as specified in RFC 1377 [MISC 6].

2. The acquisition authority shall specify the desired physical interface standards (protocol and connector) for each interface.

4. IDENTIFICATION AND REGISTRATION OF OSI OBJECTS

In order to effectively operate and administer IGOSS based systems, network addresses, MHS O/R names and other OSI objects must be uniquely identified. This section specifies the major OSI objects that must be uniquely identified and the registration mechanisms that are in effect or under development to insure unique identification.

4.1 NETWORK LAYER ADDRESSES

This section discusses the administrative and technical issues related to the assignment of Network Layer addresses. Although detailed specification of actual addressing schemes and administrative procedures are beyond the scope of this document, references are provided to other relevant sources of this information.

4.1.1 Fundamentals of NSAP Address Structure and Administration

Network Service Access Point (NSAP) addresses specify the points where the communication capability of the Network Layer (i.e., the Network Service) is made available to its users. In effect, they address the direct users of the Network Service, normally transport entities. NSAP addresses are encoded into Network Protocol Address Information (NPAI) and conveyed in the appropriate protocol data units (PDUs) between protocol entities providing the Network Service.

The basic principles of Network Layer addressing are defined in Addendum 2 to the Network service definition [ISO 5]. The first three levels of the NSAP addressing domain are standardized internationally and result in the NSAP address structure in Figure 4.1.1. The Initial Domain Part (IDP) of the address consists of two parts, the Authority and Format Identifier (AFI) and the Initial Domain Identifier (IDI). The AFI specifies the format of the IDI, the authority that is responsible for allocating IDI values, and the syntax used to represent the Domain Specific Part (DSP). The IDI is interpreted according to the value of the AFI and its value identifies the authority responsible for the structure and assignment of DSP values. The DSP is allocated and assigned by the authority specified by the IDP part.

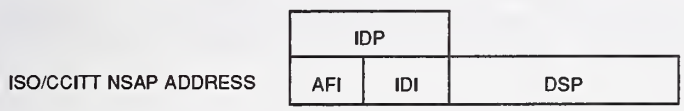


Figure 4.1.1. NSAP Address Structure.

4.1.2 Technical Requirements on NSAP Address Allocation

The design and development of an effective Network layer routing and addressing plan is fundamental to the effective acquisition and deployment of OSI Network services. Such plans guide the determination of which addressing authority(ies) are used to acquire NSAP address assignments and how the DSP portion of these addresses are structured and assigned.

The basic requirements for IGOSS NSAP addresses are specified in Part 3, clause 7 of the Workshop Agreements. In the case of the provision of the CLNS, there are numerous issues surrounding the correlation between NSAP address assignment and the correct and efficient operation of the supporting routing and data protocols that must be considered. The basic issues that need to be

considered in the development of CLNS routing and addressing plans are described in the following sources:

1. Workshop Agreements, Part 3, clauses 7 and 8.
2. The IS-IS intra-domain routing protocol [ISO 49] Annex B and section 7.1.
3. The IDRP inter-domain routing protocol [ISO 102] sections 8.1 and 8.2.
4. RFC-1237 Guidelines for OSI NSAP Allocation in the Internet [MISC 4].

4.1.3 Common IGOSS NSAP Address Authorities and DSP Formats

While technically IGOSS systems may be assigned any NSAP address that meets the requirements stated in section 4.1.1 and 4.1.2, there are small number of defined addressing schemes from which the majority of IGOSS systems will probably take NSAP Address assignments. The following table summarizes these schemes, the addressing authority, and the reference document that defines the scheme:

Table 4.1 IGOSS NSAP Addressing Schemes

Address Scheme	AFI	IDI	Addressing Authority	Reference Document
"Data Country Code USA"	39	840	American National Standards Institute	[ANSI 11]
"Data Country Code Canada"	39	124	Canadian Standards Association	[CSA 1]
"ICD 5"	47	5	US National Institute of Standards and Technology	[NIST 16]

There is a commonly used DSP structure that is supported by each of these addressing schemes. While some of these schemes may allow other DSP structures, the common structure is presented as an example. Acquisition Authorities should consult these schemes and other applicable profile documents for more information on addressing schemes.

Figure 4.1.3 depicts a DSP structure supported by each of the addressing schemes above. The following is a general description of that structure. Consult the specific reference documents for exact descriptions.

	IDP								
	AFI	IDI	DFI	Add. Author.	Reserved	Routing Domain	Area	System	NSel
Octets	1	2	1	3	2	2	2	6	1

Figure 4.1.3. Common DSP Structure.

The DSP Format Identifier (DFI) specifies the structure, semantics and administration requirements associated with the remainder of the DSP. This field provides for graceful support of multiple DSP structures should the need arise. The DFI value 80 hexadecimal identifies the DSP format described in this section.

The Address Authority field identifies the entity that is responsible for the allocation and assignment of the remaining portion of the DSP.

The Reserved field shall have a value of zero.

The Routing Domain field identifies a unique routing domain as defined in the IS-IS intra-domain routing protocol [ISO 49]. A routing domain is a coliection of ESs and ISs that, together, operate common routing protocols and are managed by a single administration.

The Area field identifies a unique subdomain of a routing domain. An area is defined in the IS-IS intra-domain routing protocol [ISO 49] as a routing subdomain which maintains detailed routing information about its own internal composition, and also maintains routing information which allows it to reach other routing subdomains.

The System field identifies a unique system (ES or IS) within an Area. The format, value, structure and meaning of this field is left to the discretion of its administrator.

The NSAP Selector field identifies a direct user of the Network Layer service, usually a Transport entity. (The NSAP Selector may also identify other direct users of the Network Service if required by the acquisition authority.) The IGOSS allows a system administrator to configure NSAP Selector-to-Transport entity mappings because, for example, several transport entities may co-exist in some systems.

4.2 MHS ORIGINATOR/RECIPIENT NAMES

The MHS Recommendations [CCITT 2-9, CCITT 28-36] identify a user to a Message Transfer Agent by means of a parameter called the Originator/Recipient Name (O/R Name). The MHS O/R Name is composed of a Directory Distinguished Name or MHS O/R address or both. O/R addresses may be of the form: Mnemonic, Numeric, Terminal or Postal. This specification mandates support for only the Mnemonic form as summarized in Table 42. Support for other O/R address forms is optional. The mnemonic address attributes which must be capable of being generated by all implementations are the country name, the administration name, private domain name, organization name, organizational units, personal name, and a list of domain-defined attributes. The value of single space should be supported for the ADMD name component of the O/R address. The private domain name attribute must also be supported by all implementations, and be included when the originator and/or the recipients are located within private domains. This information is summarized in Table 4.2.

Table 4.2 Required O/R Address Attributes

Attribute	Maximum Character Length
Country	3
ADMD	16
PRMD	16
Organization name	64
Sequence of org. units	32 each
Personal name	64
Surname	40
Given name	16
Initials	5
Generation Qualifier	3
Common name	64 (1988 MHS only)
Domain Defined Attribute List	8
Type	128
Value	

Messaging systems claiming conformance to the IGOSS shall be capable of routing on the administration name, private domain name, organization name and organizational unit attributes taken in their hierarchical order. They shall also be able to perform message delivery based on all attributes listed in Table 4.2 except in the case of DDA's which appear in MHS protocol as a constructed item "DDA.<*Type*>". They shall be tolerant of DDA's whose <*Type*> is unknown when acting as the receiving system or perform routing on it when the <*Type*> is understood. If the <*Type*>is understood, then delivery shall be performed, else a non-delivery report shall be generated. All systems shall be able to origniate messages to recipients whose O/R address contains the DDA.<*Type*> construct even though the <*Type*> is not understood by the originating messaging system.

4.3 OTHER OSI OBJECTS

All OSI applications have requirements for unique identifiers. The FTAM application must identify document types, the VT application must distinguish VT profiles and OSI Network Management requires that the managed objects be uniquely identified. An example list of other OSI objects is found in Part 6, Clause 3 of the Workshop Agreements. Moreover, certain users may have additional requirements. For example, users that employ MHS to transfer non-standard body parts or FTAM to transfer non-standard document types may want to register those body parts or document types.

4.4 REGISTRATION OF OSI OBJECTS

Authority to register network addresses, MHS addresses and other OSI objects is derived from procedural documents issued by the international standards committees [ISO 106, CCITT 49]. The registration authority that is established in these documents is hierarchical in nature - a tree structure. Pertinent components of the structure are shown in Figure 4.4. The identifier of an OSI object is described in terms of a unique path from the root of the tree to a leaf node. The identifier thus includes identifiers of all authorities responsible for the registration of the OSI object.
*

At level one of the tree, [ISO 106, CCITT 49] established branches of registration authority. They are CCITT(0), ISO(1) and joint ISO-CCITT(2). [ISO 107] specifies country code identifiers which can be assigned by the member body registration authority in the ISO arc and under the country registration in the joint ISO-CCITT arc. The identifier "840" has been assigned to the United States, and "124" has been assigned to Canada. [ISO 108] gives the procedures for delegating registration authority to identified organizations that are not ISO member bodies.

The International Code Designator component of the Network address may be assigned under the ISO arc by an organization that has been delegated registration authority according to [ISO 108]. ICD assignments have been made to NIST (ICD 5) and to the OSE Implementors Workshop (ICD 14) under this authority. The General Services Administration has the operational responsibility of assigning the Address Authority component of the Network address to U.S. government and non-government organizations under the authority delegated to NIST under ICD 5.

An MHS O/R address is encoded as a set of hierarchically ordered attributes (see Section 4.2). The attributes include Country, Administration Domain, Private Domain and Organization Name. An MHS O/R Name may have an Administration Domain attribute, a Private Management Domain attribute, or both. An Address Registration Authority is needed to register certain components of an MHS O/R Name. ANSI has established a MHS management domain (MD) name registration service which was mutually agreed between ANSI and the Department of State. Any MHS management domain name value registered directly with ANSI is understood to be nationally unique when used in conjunction with country = US. As such, ANSI is the U.S. national MHS MD name registration authority. All values registered in this registry are registered subordinate to the US sub-arc under the joint ISO-CCITT arc as illustrated in Figure 4.4. All ADMD name values shall be registered directly with ANSI, PRMD name values may be, too. Private Domains and Administration Domains will assign unique organization names to users of their services and delegate to the organization indicated by the organization names, the authority to assign organizational unit and personal names.

Any MD name registered directly with ANSI may establish itself as a registration subauthority. For example, GSA offers MD name registration services under the Registration Authority name "GOV". However, to assure its uniqueness in MHS, the identity of the authority (s) between ANSI and the registrant, must also be included in the MD name value. This shall be achieved by using the

construction syntax specified in the ANSI registration procedure guidelines. For example, in the case of GSA, being a sub-authority registrar, the requested MD name "AAA" would appear as "GOV+AAA" when used as a PRMD name value in MHS O/R address.

Other OSI objects (i.e., those identified in Part 6 of the Workshop Agreements) are assigned under ICD 14. Under this authority, the OSE Implementors' Workshop has delegated authority to each SIG to assign object identifiers to objects of interest to that SIG. Consult Part 6 of the Workshop Agreements for additional information.

Detailed registration procedures will be specified in companion documents issued by each IGOSS organization.

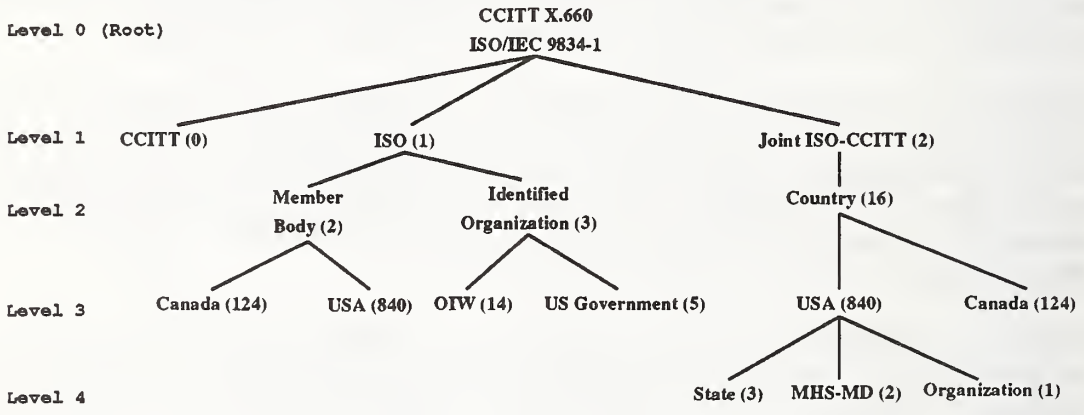


Figure 4.4. Registration Authority Hierarchy.

5. PROCUREMENT CONSIDERATIONS

Procuring information systems for deployment in multi-vendor computer networks involves a complex set of issues: specification of protocol requirements, wording of solicitations, determination of conformance against the specification and of interoperability among conformant products, assessment of the function and performance of products against the solicitation requirements, extension of standards-based products to meet user requirements when no standard solution is available, and more. While the IGOSS addresses solely the specification of protocol requirements, additional assistance is available to the acquisition authority, both now and in the future. The following sections refer the acquisition authority to appropriate sources of such assistance.

5.1 USER'S GUIDE

Acquisition Authorities should not use the IGOSS without understanding the broad issues surrounding the specification; and, of course, the issues are different for executives, managers, technical professionals, and procurement officials. A guide discussing the relevant issues for each category of user, and in a language that each type of user can understand, is planned by the IGOSS partners. Until this IGOSS User's Guide is available, acquisition authorities can consult an existing user's guide published by one of the IGOSS partners [NIST 7].

5.2 EVALUATION GUIDELINES

The IGOSS mandates for each protocol a minimum set of functions to meet general user requirements. In many instances, additional functions might be supported within the Workshop Agreements and/or the protocol standards. The acquisition authority must determine and specify such additional functions that are required within an acquisition. The acquisition authority is responsible for determining that the vendor products proposed meet any and all functional requirements.

IGOSS does not cite performance criteria. Note that protocol definitions include quality of service parameters and other tunable functions. The acquisition authority must determine and specify those performance-related features that are desired to be under user or application process control and those desired to be under system operator control. The acquisition authority may also wish to specify benchmarking criteria as evidence of satisfying specific performance requirements.

One of the IGOSS partners has issued "Guidelines for the Evaluation of Message Handling Systems Implementations" [NIST 9], "Guidelines for the Evaluation of File Transfer, Access, and Management Implementations" [NIST 10], and "Guidelines for the Evaluation of Virtual Terminal Implementations" [NIST 15] to assist users and acquisition authorities in evaluating the degree to which implementations of those applications meet the specific performance and functional requirements of a procurement. Further guidelines are planned.

5.3 TESTING

Use of a specification based on standards, while bringing many benefits, creates a new problem for acquisition authorities: how can vendor claims of conformance be verified? In the case of IGOSS, because it involves standards for communication between systems, an additional problem faces the acquisition authority: how can interoperability among conforming products be assured? The IGOSS

partners accept the responsibility for providing tools to enable the acquisition authority to answer these questions as efficiently and cheaply as possible.

The IGOSS partners will develop a testing program leading to the public availability of lists and databases of conforming and interoperable products. The resulting information will be freely available to all users or potential users of the IGOSS or products meant to conform to the IGOSS. In the interim, one of the IGOSS partners has already laid a significant foundation for such a testing program. Prospective users of the IGOSS specification, as well as users of the existing profiles: MAP, TOP, UCA, and GOSIP, can make use of the conformance and interoperability information available through the GOSIP Testing Program [NIST 8]. The IGOSS partners envision that testing requirements will be driven largely by user demand; therefore, to increase the amount and value of testing information available, users are encouraged to require prospective vendors to demonstrate conformance and interoperability by following the procedures already established by NIST, and to indicate to prospective vendors, an intent to adopt the procedures that evolve as the IGOSS partners establish an IGOSS Testing Program.

5.4 CHARACTER SET SUPPORT

In OSI based products, each Application layer service provides support for specific ISO standard character sets. Part 21 of the Workshop Agreements specifies the character set support requirements for each application.

Currently IA5 Text commonly known as ASCII is commonly supported by all major vendors and is the character set of choice for application compatibility. In addition, many OSI applications also support other character sets such as ISO 646, 6937, 8859 and CCITT character sets such as T.61 and T.71. Acquisition authorities should specify their requirements for any character set support that is beyond that mandated by the Workshop Agreements.

Currently, character set support is based on harmonized Workshop Agreements and ISO JTC1 SGFS. In the future, it is expected that applications will support worldwide languages using the ISO 10646 character set standard. The IS 10646 standard is aligned to industry use of the UNICODE character representation which covers all language and alphabet representations worldwide.

5.5 VENDOR ENHANCEMENTS

It is expected that most vendors will update their products, for example, from a Draft International Standard version to an International Standard version, as implementation specifications are completed in the Workshop Agreements. Also, some vendors may provide additional functionality. Implementations that go beyond the functional units stated in Section 3 must be implemented according to the Workshop Agreements and must interwork with implementations that strictly comply with Section 3. Requests For Proposals should encourage vendor enhancements, where required to meet user needs, as a preferred alternative to using the required, but missing, functions as a justification for procuring redundant protocols.

REFERENCES

American National Standards Institute

1. Integrated Services Digital Network - Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT-Layer 1 Specification, ANS T1.601-1988.

2. Integrated Services Digital Network - Basic Access Interface at S and T Reference Points - Layer 1 Specification, ANS T1.605-1988.

3. Carrier to Customer Installation - DS1 Metallic Interface, ANSI T1. 403-1989.

4. American National Standard Information Retrieval Application - Service Definition and Protocol Specification for Open Systems Interconnection, ANSI Z39.50-1992.

5. Information Processing Systems - Computer graphics - Metafile for the storage and transfer of picture description information, ANSI/ISO 8632.

6. American National Standard - Digital Representation for Communication of Product Definition Data, ANSI Y14.26M-1989.

7. American National Standard - Information Retrieval - Application Service Definition and Protocol Specification for Open Systems Interconnection, ANSI Z39.50.

8. American National Standard for Information Systems - Computer Graphics - X Window System Data Stream Definition, ANSI X3.196-199X.

9. ANS T1.617 - DSS1 - Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service, 1991

10. ANS T1.618 - DSS1 - Signaling Specification for Frame Relay Bearer Service, 1991

11. ANS X3.216 - Structure and Semantics of the Domain Specific Part (DSP) of the OSI Network Service Access Point (NSAP) Address.

12. ANS X3.229 - 199X - Fiber Distributed Data Interface (FDDI) Station Management (SMT). (ANSI X3T9 approved SMT Version 7.2)

Canadian Standards Association

1. CSA Z243.110.2 Canadian OSI Registration Procedures and Guidelines - Part 2 -Guidelines for Network Service Access Point Addresses for the Data Country Code Format.

Electronic Industries Association

Interface between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange, EIA-232C.

Institute of Electrical and Electronics Engineers, Inc.

1. Standard for Information Technology -- OSI Application Program Interface - Common ASN.1 Object Management API for X.400 and Directory Services APIs, P1224.

2. Standard for Information Technology -- OSI Application Program Interfaces -- X.400 Based Electronic Messaging API, P1224.1.

3. Standard for Information Technology, Portable Operating System Interface (POSIX) -- Directory Services Application Programming Interface, P1003.17.

4. Draft Standard 802.1B: LAN/MAN Management, P802.1B/D20, January 27, 1992.

5. Draft Supplement to IEEE Std. 802.3: Repeater Management, P802.3.K/D5, December 22, 1991.

The above documents may be obtained from: IEEE Standards Office, 345 East 47th Street, New York, N.Y. I00I7. Phone (800) 678-4333.

International Organization for Standardization

NOTE: Several versions of some of the ISO references that follow may exist. Different versions of the same reference are distinguished by the year of publication. The reader should consult the appropriate section of the Workshop Agreements to determine the applicable version when a date is not provided.

1. Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Ref. No. ISO 7498-1984(E).

2. Information Processing Systems - Data Communications - Use of X.25 to provide the OSI Connection Mode Network Service, ISO 8878.

3. Information Processing Systems - Open Systems Interconnection - Network Service Definition, ISO 8348.

4. Information Processing Systems - Open Systems Interconnection - Addendum to the Network Service Definition Covering Connectionless Data Transmission, ISO 8348 Addendum 1.

5. Information Processing Systems - Open Systems Interconnection - Addendum to the Network Service Definition Covering Network Layer Addressing, ISO 8348 Addendum 2.

6. Information Processing Systems - Open Systems Interconnection - Internal Organization of the Network Layer, ISO 8648.

7. Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless Network Service, ISO 8473.

8. Information Processing Systems - Open Systems Interconnection - Data Communication - X.25 Packet Level Protocol for Data Terminal Equipment, ISO 8208.

9. 7-bit Coded Character Set for Information Processing Interchange, ISO 646, I973.

10. Information Interchange - Representation of Local Time Differentials, ISO 3307, I975.

11. Information Processing Systems - Open Systems Interconnection - Working Draft - End System to Intermediate System Routing Exchange Protocol for use in Conjunction with ISO 8473.

12. Information Processing Systems - Open Systems Interconnection - Transport Service Definition, ISO 8072.

13. Information Processing Systems - Open Systems Interconnection - Transport Protocol Specification, ISO 8073.

14. Information Processing Systems - Open Systems Interconnection - Session Service Definition, ISO 8326.

15. Information Processing Systems - Open Systems Interconnection - Session Protocol Specification, ISO 8327.

16. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 1: General Introduction, ISO 8571-1.

17. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 2: The Virtual Filestore Definition, ISO 8571-2.

18. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 3: File Service Definition, ISO 8571-3.

19. Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management Part 4: File Protocol Specification, ISO 8571-4.

20. Information Processing Systems - Open Systems Interconnection - Connection-Oriented Presentation Service Definition, ISO 8822.

21. Information Processing Systems - Open Systems Interconnection - Connection-Oriented Presentation Protocol Specification, ISO 8823.

22. Information Processing Systems - Open Systems Interconnection - Service Definition for Association Control Service Element - Part 2: Association Control, ISO 8649.

23. Information Processing Systems - Open Systems Interconnection - Protocol Specification for Association Control Service Element: Association Control, ISO 8650.

24. Information Processing Systems - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), ISO 8824.

25. Information Processing Systems - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), ISO 8825.

26. Information Processing Systems - Data Communications - High-Level Data Link Control Procedures - Description of the X.25 LAPB-compatible DTE Data Link Procedures, ISO 7776.

27. Information Processing Systems - Data Interchange - Structures for the Identification of Organizations, ISO 6523, 1984.

28. Information Processing Systems - Local Area Networks - Part 2: Logical Link Control, ISO 8802/2.

29. Information Processing Systems - Local Area Networks - Part 3: Carrier Sense Multiple Access With Collision Detection, ISO 8802-3

30. Information Processing Systems - Local Area Networks - Part 4: Token-passing Bus Access Method and Physical Layer Specifications, ISO 8802/4.

3l. Information Processing Systems - Local Area Networks Part 5: Token Ring Access Method and Physical Layer Specifications, ISO 8802/5.

32. Information Processing Systems - Open Systems Interconnection - Virtual Terminal Services - Basic Class, ISO 9040.

33. Information Processing Systems - Open Systems Interconnection - Virtual Terminal Protocol - Basic Class, ISO 9041.

34. Information Processing Systems - Open Systems Interconnection. Virtual Terminal Service, Basic Class, ISO 9040, Addendum 1, 1988.

35. Information Processing Systems - Open Systems Interconnection, Virtual Terminal Protocol, Basic Class, ISO 9041, Addendum 1, 1988.

36. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 1: Introduction and General Principles, ISO 8613-1.

37. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 2: Document Structures ISO 8613-2.

38. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 4: Document Profile, ISO 8613-4.

39. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 5: Office Document Interchange Format (ODIF), ISO 8613-5.

40. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 6: Character Content Architectures, ISO 8613-6.

41. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 7: Raster Graphics Content Architectures, ISO 8613-7.

42. Information Processing - Text and Office Systems-Office-Document Architecture (ODA) and Interchange Format - Part 8: Geometric Graphics Content Architectures, ISO 8613-8.

43. Information Processing Systems - Protocol Identification in the Network Layer, DTR 9577.

44. Information Processing Systems - End System to Intermediate System Routing Exchange Protocol for use with ISO 8473, ISO 9542.

45. Information Processing Systems - Data Communications - Provision of the OSI Connection-mode Network Service, by Packet Mode Terminal Equipment connected to an Integrated Services Digital Network (ISDN), ISO 9574.

46. Information Processing Systems - Transport Service Definition covering Connectionless Mode Transmission, ISO 8072/ADD.

47. Information Processing Systems - Protocol for Providing the Connectionless Mode Transport Service, ISO 8602.

48. Information Processing Systems - Telecommunications and Information Exchange Between Systems -OSI Routing Framework, ISO/TR 9575.

49. Information Processing Systems - Telecommunications and Information Exchange Between Systems -Intermediate systems to Intermediate system Intra-Domain routing exchange protocol for use in conjunction with the protocol for providing the Connectionless mode Network Service ISO 10589.

50. Information Processing Systems - Text Communication - Remote Operations, Part 1: Model, Notation and Service Definition, ISO 9072-1

51. Information Processing Systems - Text Communication - Remote Operations, Part 2: Protocol Specification, ISO 9072-2.

52. Information Processing Systems - Text Communication - Reliable Transfer, Part 1: Model and Service Definition, ISO 9066-1.

53. Information Processing Systems - Text Communication - Reliable Transfer, Part 2: Protocol Specification, ISO 9066-2.

54. Information Processing Systems - Open Systems Interconnection - Service Definition of Common Application Service Elements - Commitment, Concurrency and Recovery, ISO 9804.

55. Information Processing Systems - Open Systems Interconnection - Specification of Protocols for Common Application Service Elements - Commitment Concurrency and Recovery, ISO 9805.

56. Information Processing Systems - Open Systems Interconnection - Connectionless ACSE Protocol to Provide the Connectionless - Mode ACSE Service, ISO 10035.

57. Information Processing Systems - Open Systems Interconnection - Connectionless Presentation Protocol to Provide the Connectionless-Mode Presentation Service, ISO 9576.

58. Information Processing Systems - Open Systems Interconnection - Connectionless Session Protocol to Provide the Connectionless-Mode Session Service, ISO 9548.

59. Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing -Part 1: Model, ISO 10026-1.

60. Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing -Part 2: Service, ISO 10026-2.

61. Information Processing Systems - Open Systems Interconnection - Distributed Transaction Processing -Part 3: Protocol, ISO 10026-3.

62. Information Processing Systems - Open Systems Interconnection - Remote Database Access - Part 1: Generic Model, Service, and Protocol, ISO 9579-1, 1993.

63. Information Processing Systems - Remote Database Access Part 2: SQL Specialization, ISO 9579-2, 1993.

64. Industrial Automation Systems - Manufacturing Message Specification Part 1: Service Definition, ISO 9506-1.

65. Industrial Automation Systems - Manufacturing Message Specification Part 2: Protocol Specification, ISO 9506-2.

66. Information and Documentation - Search and Retrieve Application Service Definition for Open Systems Interconnection, ISO 10162.

67. Information and Documentation - Search and Retrieve Application Protocol Specification for Open Systems Interconnection, ISO 10163.

68. Information Technology - Database Language - SQL - ISO 9075, 1992.

69. Information and Documentation - International Standard Profile - Application Profile for Search and Retrieval - Connection-oriented, ISO SC4 WG4 ALD11.

70. Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models, and Service ISO 9594-1.

71. Information Technology - Open Systems Interconnection - The Directory: Models, ISO 9594-2.

72. Information Technology - Open Systems Interconnection - The Directory: Abstract Service Definition ISO 9594-3.

73. Information Technology - Open Systems Interconnection - The Directory: Procedures for Distributed Operation, ISO 9594-4.

74. Information Technology - Open Systems Interconnection - The Directory: Protocol Specifications, ISO 9594-5.

75. Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types, ISO 9594-6.

76. Information Technology - Open Systems Interconnection - The Directory: Selected Object Classes, ISO 9594-7.

77. Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, ISO 9594-8.

78. Information Technology - Open Systems Interconnection - The Directory: Replication, ISO 9594-9.

79. Information Technology - Open Systems Interconnection - Management Information Service Definition -Common Management Information Service Definition, ISO 9595.

80. Information Technology - Open Systems Interconnection - Management Information Protocol Specification - Common Management Information Protocol, ISO 9596-1.

81. Information Technology - Open Systems Interconnection - Structure of Management Information - Part 2: Definitions of Management Information, ISO 10165-2.

82. Information Technology - Telecommunications and information exchange between systems - Elements of Management Information Related to OSI Network Layer Standards, Revised text for ISO DIS 10733, September 26, 1991.

83. Information Technology - Telecommunications and information exchange between systems - Intermediate system to Intermediate system Intra-Domain routing information exchange protocol for use in conjnction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473), ISO 10589: 1992(E).

84. Information Technology - Telecommunications and information exchange between systems - Elements of Management Information Related to OSI Transport Layer Standards, ISO JTC1/SC6 N6784, November 7, 1991. (DIS Ballot text for ISO DIS 10737-1)

85. Information Technology - Open Systems Interconnection - Structure of Management Information - Part 4: Guidelines for the Definition of Managed Objects, ISO 10165-4.

86. Information Technology - Open Systems Interconnection - Systems Management - Part 1: Object Management Function, ISO 10164-1.

87. Information Technology - Open Systems Interconnection - Systems Management - Part 2: State Management Function, ISO 10164-2.

88. Information Technology - Open Systems Interconnection - Systems Management - Part 3: Attributes for Representing Relationships, ISO 10164-3.

89. Information Technology - Open Systems Interconnection - Systems Management - Part 4: Alarm Reporting Function, ISO 10164-4.

90. Information Technology - Open Systems Interconnection - Systems Management - Part 5: Event Report Management Function, ISO 10164-5.

91. Information Technology - Open Systems Interconnection - Systems Management - Part 6: Log Control Function, ISO 10164-6.

92. Information Technology - Open Systems Interconnection - Systems Management - Part 7: Security Alarm Reporting Function, ISO 10164-7.

93. Information Technology - Open Systems Interconnection - Service definition for the Association Control Service Element - ADDENDUM 1: Peer-entity authentication during association establishment, ISO 8649 DAD 1.

94. Information Technology - Open Systems Interconnection - Protocol specification for the Association Control Service Element - ADDENDUM 1: Peer-entity authentication during association establishment, ISO 8650 DAD 1.

95. Information Processing Systems - Fiber Distributed Data Interface (FDDI) Part 1: Token Ring Physical Layer Protocol, ISO 9314-1.

96. Information Processing Systems - Fiber Distributed Data Interface (FDDI) Part 2: Token Ring Medium Access Control (MAC), ISO 9314-2.

97. Information Processing Systems - Fiber Distributed Data Interface (FDDI) Part 3: Token Ring Physical Medium Dependent (PMD), ISO 9314-3

98. Information Processing Systems - Fiber Distributed Data Interface (FDDI) Part 4: Token Ring Single Mode Fiber Physical Medium Dependent (SMF-PMD), CD 9314-4.

99. Information Processing Systems - Fiber Distributed Data Interface (FDDI) Part 6: Token Ring Station Management (SMT) Medium Dependent (MAC), CD 9314-6.

100. Information Technology - Telecommunications and information exchange between systems - End System Routing Information Exchange Protocol for use in conjunction with ISO 8878, ISO 10030.

101. Protocol Combinations to Provide and Support the OSI Network Service - Provision and Support of the Connectionless Mode Network Service, ISO 8880-3.

102. Information Processing Systems - Telecommunications and Information Exchange Between Systems -Protocol for Exchange of Inter-Domain Routing Information among Intermediate Systems to Support Fowarding of ISO 8473 PDUs, CD 10747.

103. Information Processing Systems- Telecommunications and Information Exchange between Systems - MAC Sublayer Interconnection (MAC Bridging), ISO 10038.

104. Information Processing Systems - Open Systems Interconnection - International Standardized Profile 12061 - Transaction Processing.

    a) ISO ISP 12061-5, ATP 11: Polarized Application Supported Transactions
    b) ISO ISP 12061-7, ATP 21: Unchained Provider Supported Transactions
    c) ISO ISP 12061-9 ATP 31: Chained Provider Supported Transactions

105. Standard for the Exchange of Product Model Data (STEP), ISO 10303.

106. Procedures for the operation of OSI Registration Authorities, General Procedures, ISO 9834-1, 1992

107. Codes for the Representation of Names of Countries, ISO 3166, 1988

108. Data Interchange - Structure for the Identification of Organizations, ISO 6523, 1984.

109. Information Processing Systems - Computer Graphics - Metafile for the Storage and Transfer of Picture Description Information, ISO 8632:1992.

110. Information Technology - International Standardized Profile 11187-4 - AVT1n, AVT2n - Virtual Terminal Basic Class - Application Profile - Part 4: AVT23 - S mode Paged Application Profile.

111. Information Technology - International Standardized Profile 10611, Parts 1-5 - AMH1n - Message Handling Systems - Common Messaging.

112. Information Technology - International Standardized Profile 11188-3 - Common Upper Layer Requirements - Part 3 - Minimal OSI Upper Layer Facilities.

The above documents may be obtained from:

ANSI Sales Department
1430 Broadway
New York, NY 10018
(212) 642-4900

International Telephone and Telegraph Consultative Committee

1. CCITT Recommendation X.25-1984, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks.

2. CCITT Recommendation X.400, (Red Book, 1984), Message Handling Systems: System Model-Service Elements.

3. CCITT Recommendation X.401, (Red Book, 1984), Message Handling Systems: Basic Service Elements and Optional User Facilities.

4. CCITT Recommendation X.408, (Red Book, 1984), Message Handling Systems: Encoded Information Type Conversion Rules.

5. CCITT Recommendation X.409, (Red Book, 1984), Message Handling Systems: Presentation Transfer Syntax and Notation.

6. CCITT Recommendation X.410, (Red Book, 1984), Message Handling Systems: Remote Operations and Reliable Transfer Server.

7. CCITT Recommendation X.411, (Red Book, 1984), Message Handling Systems: Message Transfer Layer.

8. CCITT Recommendation X.420, (Red Book, 1984), Message Handling Systems: Interpersonal Messaging User Agent Layer.

9. CCITT Recommendation X.430, (Red Book, 1984), Message Handling Systems: Access Protocol for Teletex Terminals.

10. CCITT Recommendation X.214, (Red Book, 1984), Transport Service Definition for Open Systems Interconnection for CCITT Applications.

11. CCITT Recommendation X.224, (Red Book, 1984), Transport Protocol Specification for Open Systems Interconnection for CCITT Applications.

12. CCITT Recommendation X.215 (Red Book, 1984), Session Service Definition for Open Systems Interconnection for CCITT Applications.

13. CCITT Recommendation X.225 (Red Book, 1984), Session Protocol Specification for Open Systems Interconnection for CCITT Applications.

14. CCITT Recommendation X.400 - Series Implementor's Guide (Version 6, November 1987).

15. CCITT Recommendation X.121 (Red Book, 1985), International Numbering Plan for Public Data Networks.

16. CCITT Recommendation V.35 - Data Transmission at 48 kilobits/second using 60-108 kHz group band circuits.

17. CCITT Recommendation T.410 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Overview

18. CCITT Recommendation T.411 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Introduction and General Principles

19. CCITT Recommendation T.412 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Document Structures

20. CCITT Recommendation T.414 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Document Profile

21. CCITT Recommendation T.415 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Document Interchange Format (ODIF)

22. CCITT Recommendation T.416 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Character Content Architectures

23. CCITT Recommendation T.417 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Raster Graphics Content Architectures.

24. CCITT Recommendation T.418 (Blue Book, 1988) Open Document Architecture (ODA) and Interchange Format - Geometric Graphics Content Architectures.

25. CCITT Recommendation Q.921 (I.441) (Blue Book, 1988) ISDN User-Network Interface Data Link Layer Specification.

26. CCITT Recommendation Q.931 (I.451) (Blue Book, 1988) ISDN User-Network Interface Layer 3 Specification for Basic Call Control.

27. CCITT Recommendation X.31 (Blue Book, 1988) Support of Packet Mode Terminal Equipment by an ISDN.

28. CCITT Recommendation X.400 (Blue Book, 1988), Message Handling System and Service Overview. This Recommendation is identical to CCITT Recommendation F.400 (Blue Book, 1988).

29. CCITT Recommendation X.402 (Blue Book, 1988), Message Handling Systems: Overall Architecture.

30. CCITT Recommendation X.403 (Blue Book, 1988), Message Handling Systems: Conformance Testing.

31. CCITT Recommendation X.407 (Blue Book, 1988), Message Handling Systems: Abstract Service Definition Conventions.

32. CCITT Recommendation X.408 (Blue Book, 1988), Message Handling Systems: Encoded Information Type Conversion Rules.

33. CCITT Recommendation X.411 (Blue Book, 1988), Message Handling Systems: Message Transfer System: Abstract Service Definition and Procedures.

34. CCITT Recommendation X.413 (Blue Book, 1988), Message Handling Systems: Message Store: Abstract Service Definition.

35. CCITT Recommendation X.419 (Blue Book, 1988), Message Handling Systems: Protocol Specifications.

36. CCITT Recommendation X.420 (Blue Book, 1988), Message Handling Systems: Interpersonal Messaging System.

37. CCITT Recommendation X.500 (December 1992), Information Technology - Open System Interconnection - The Directory: Concepts, Models and Services (Technically aligned with ISO 9594-1).

38. CCITT Recommendation X.501 (December 1992), Information Technology - Open System Interconnection - The Directory: Models (Technically aligned with ISO 9594-2).

39. CCITT Recommendation X.509 (December 1992), Information Technology - Open System Interconnection - The Directory: Authentication Framework (Technically aligned with ISO 9594-8).

40. CCITT Recommendation X.511 (December 1992), Information Technology - Open System Interconnection - The Directory: Abstract Service Definition (Technically aligned with ISO 9594-3).

41. CCITT Recommendation X.518 (December 1992), Information Technology - Open System Interconnection - The Directory: Procedures for Distributed Operation (Technically aligned with ISO 9594-4).

42. CCITT Recommendation X.519 (December 1992), Information Technology - Open System Interconnection - The Directory: Protocol Specifications (Technically aligned with ISO 9594-5).

43. CCITT Recommendation X.520 (December 1992), Information Technology - Open System Interconnection - The Directory: Selected Attribute Types (Technically aligned with ISO 9594-6).

44. CCITT Recommendation X.521 (December 1992), Information Technology - Open System Interconnection - The Directory: Selected Object Classes (Technically aligned with ISO 9594-7).

45. CCITT Recommendation X.525 (December 1992), Information Technology - Open System Interconnection - The Directory: Replication (Technically aligned with ISO 9594-9).

46. CCITT Recommendation F.435 - Message Handling Systems: EDI Messaging Service (1991).

47. CCITT Recommendation X.435 - Message Handling Systems: EDI Messaging System (1991).

48. CCITT Draft Recommendation (M.gnm) Generic Network Information Model, November 1991.

49. CCITT Recommendation X.660 (1992), Procedures for the Operation of OSI Registration Authorities, General Procedures.

The above documents may be obtained from: International Telecommunications Union, Place des Nations, CH I2II, Geneve 20 SWITZERLAND.

National Communications System

Federal Standard FED-STD 1041, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) For Operation With Packet-Switched Data Communications Networks, National Communications System.

National Institute of Standards and Technology

1. NIST Special Publication 500-206, Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 6, December 1992. This document can be purchased from National Technical Information Service (NTIS), U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. For telephone orders call: (703) 487-4650. For information on how to access this document on-line, contact Brenda Gray at (301) 975-3664.

2. FIPS Pub 107, Local Area Networks: Baseband Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Specifications and Link Layer Protocol, NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22I6I.

3. FIPS Pub 100-1, Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) For Operation With Packet-Switched Data Networks, (PDSN), or between two DTEs, by Dedicated Circuit. NTIS, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22I6I.

4. FIPS Pub 179, Government Network Management Profile (GNMP). See [NIST 7] for ordering information.

5. Military Supplement to ISO Transport Protocol, National Institute of Standards and Technology, National Computer Systems Laboratory, ICST/SNA-85-17, 1985.

6. Implementation Guide for ISO Transport Protocol, National Institute of Standards and Technology, National Computer Systems Laboratory, ICST/SNA-85-18, 1985.

7. NIST Special Publication 500-192 Government Open Systems Interconnection User's Guide, Version 2. This document can be purchased from the National Technical Information Service (NTIS), U. S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. For telephone orders call (703) 487-4650.

8. GOSIP Conformance and Interoperation Testing and Registration, March 1991, Version 1.0, NISTIR 4594. The document can be obtained from NIST, Systems & Network Architecture Division, Automated Methods Group, Bldg 225, Room B217, Gaithersburg, MD 20899.

9. NIST Special Publication 500-182, Guidelines for the Evaluation of Message Handling Systems Implementations. See [NIST 7] for NTIS ordering information.

10. NIST Special Publication 500-196, Guidelines for the Evaluation of File Transfer, Access and Management Implementations. See [NIST 7] for NTIS ordering information.

11. FIPS Pub 128, Computer Graphics Metafile (CGM).

12. FIPS Pub 152, Information Processing - Text and office systems - Standard Generalized Markup Language (SGML) - Aligned with ISO 8879.

13. Working Implementation Agreements for Open Systems Interconnection Protocols, March 1992.

14. "Specifications for a Secure Hash Standard," proposed Federal Information Processing Standard, January 22, 1992 (available from NIST, call 301-975-2816.

15. NIST Special Publication 500-205, Guidelines for the Evaluation of Virtual Terminal Implementation. See [NIST 7] for NTIS ordering information.

16. FIPS 146-1, Government Open Systems Interconnection Profile (GOSIP), Version 2. See [NIST 7] for NTIS ordering information.

Miscellaneous

1. Manufacturing Automation Protocol

2. Technical and Office Protocols, Specification Version 3.0

For copies of the two documents listed above, contact: Corporation for Open Systems, 8260 Willow Oaks Corporate Drive, Suite 700, Fairfax, VA 22031.

3. RFC 1331, Point-to-Point Protocol for the transmission of multi-protocol datagrams over Point-to-Point links, D. Perkins, July 1990.

4. RFC 1237 Guidelines for OSI NSAP allocation in the Internet, R. Colella, E.P. Gardner, R.W. Callon, July 1991.

5. RFC 1172, The Point-to-Point Protocol (PPP) Initial Configuration Options, D. Perkins, R. Hobby

6. RFC 1377, The PPP OSI Network Layer Control Protocol (OSINLCP), November 1992.

Copies of the four documents listed above can be obtained from the Internet Network Information Center (NIC).

7. X-Window System, X Version 11 R4 (X11-R4).

8. Z39.50 Implementors Group Profile, ANSI Z39.50-MA-026.

9. Network Management Forum: Forum 006, "*Forum Library - Volume 4: OMNIPoint 1 Definitions*," Issue 1.0, August 1992.

FOREWORD TO THE APPENDICES

Appendices 1-5 describe IGOSS requirements for which adequate specifications have yet to be developed. The appendices give a summary of protocols planned for inclusion in a future version of the IGOSS. Where appropriate, the requirements for including the protocol and a plan of work to meet the requirements are given. It is expected that this information can assist IGOSS organizations in planning decisions related to the acquisition of implementations of OSI protocols.

Appendix 6 specifies conformance specifications for the Directory Services application. Appendix 7 contains the meaning of a list of acronyms used in this document.

APPENDIX 1. SECURITY

1.1 BACKGROUND

The Open Systems Interconnection (OSI) Security Architecture was approved as an International Standard (iS 7498/2) in 1988. It defines a general architecture that may be used in providing security services in OSI networks. Five primary security services, authentication, access control, data confidentiality, data integrity, and non-repudiation, are specified in the architecture. It also discusses mechanisms that may be used in providing these services and the OSI layers where they could be offered. IS 7498/2 provides a framework for the incorporation of security in OSI protocols, but significant effort is required to standardize protocol specifications that contain security features. This appendix addresses the need for security standards, the status of standards being developed and plans for developing additional required standards.

While OSI attempts to improve communications between heterogeneous computer systems, there is a need to limit access to only authorized users and for authorized purposes. Systems that process sensitive data must be protected from a wide variety of threats. The security services mentioned above provide safeguards against unauthorized access to systems and data, and against unauthorized disclosure, modification or destruction of data, which may occur accidentally or intentionally.

Security services may be provided at one or more of the layers 3, 4, and 7. The security architecture described here suggests a range of choices for security services and their placement. It is expected that subsets of these services at selected layers will adequately satisfy specific security requirements. Security may restrict access and may inhibit interoperability, thus the selection and placement of security mechanisms should insure that interoperability among components of the target system is not affected.

1.2 REQUIREMENTS

The security services defined in the OSI security architecture are authentication, access control, confidentiality, integrity and non-repudiation. These are defined in detail in IS 7498/2 and are summarized below:

- **Data confidentiality** services protect against unauthorized disclosure. Protection of medical records to insure patient's privacy is an example of the need for confidentiality.

- **Data integrity** services protect against unauthorized modification, insertion and deletion. Electronic funds transfer between banks requires protection against modification of the information.

- **Authentication** services verify the identity of communicating peer entities and the source of data. Owners of bank accounts require assurance that money will be withdrawn only by them.

- **Access control** services allow only authorized communications and access to system resources. Only financial officers are authorized access to a company's financial plans.

- **Non-repudiation**, with proof of origin, provides to the recipient proof of the origin of data and protects against any attempt by the originator to falsely deny sending the data. Non-repudiation, with proof of delivery, provides to the sender proof of the delivery of data. The non-repudiation

service can be used to prove to a judge that a person received or sent a message (e.g., a purchase order).

Government agencies may require the implementation of some or all of these services in their communications systems. Authentication, confidentiality, integrity, and access control services may be implemented in layers 3, 4 and 7 of the OSI architecture. The non-repudiation service is offered only at layer 7. It is possible to provide comparable security services at layers 3 and 4, such services should be required at only one of these layers. The selection of security services at specific layers must be made by the acquisition authority. The selection and placement of mechanisms to support security services is based on the perceived threats and a balance between protection and cost.

1.3 STATUS

Interoperability standards for IGOSS security are required at layers 3, 4, and 7 of the OSI architecture. NIST published the Secure Data Network System (SDNS) specifications for security at layers 3 and 4. (See NISTIR 90-4250). ANSI presented these specifications to ISO, where they are being progressed as the Network Layer Security Protocol (NLSP) and the Transport Layer Security Protocol (TLSP). In Canada, the COSAC security profile provides a guide to implementing security consistent with the OSI Security Architecture (IS 7498/2). Specifications for data authentication have been issued in standards by the National Institute of Standards and Technology (FIPS 113) and ANSI (ANSI X9.9). Specification for a DES-based key management protocol has been issued in a standard by ANSI (X9.17). The U.S. FederalGovernment is promulgating a new Standard Security Label (SSL) FIPS which provides a security labeling mechanism which will be referenced by the GOSIP. Security Functional Groups for the X.400 Message Handling System defining three security classes are now specified in the Workshop Agreements and referenced by the IGOSS. The following subsections highlight current efforts in standardization of security protocols and estimated time frames for the availability of standards.

1.3.1 OSI Security Frameworks

A set of security frameworks on specific security services and procedures are planned by the ISO/ JTC1/SC21/WG1 Security Group. Although the scope of these frameworks is broader than just OSI, the Security SIG will continue to use them as guidance in the adoption of Implementors Agreements.

1.3.2 Network Layer Security

The SDNS Security Protocol for Layer 3 document (SP3) is available for public use. This protocol was presented to ANSI in 1989, who then submitted it to ISO as a U.S. contribution. ISO is currently progressing a Network Layer Security Protocol (NLSP) that is based on the original SP3. Both SP3 and NLSP encapsulate Network Protocol Data Units (N-PDUs) and provide different levels of protection for use with connection oriented and connectionless network protocols. These protocols may be implemented in intermediate and end systems. The Network Layer Security Protocol (NLSP) became an International Standard (IS) in late 1993.

1.3.3 Transport Layer Security

The SDNS Security Protocol for Layer 4 document (SP4) is available for public use. This protocol was presented to ANSI in 1989, who then submitted it to ISO as a U.S. contribution. A Transport Layer Security Protocol (TLSP) that is based on the original SP4 is now an ISO international standard. Both SP4 and TLSP encapsulate Transport Protocol Data Units (T-PDUs) as a SE T-PDU (SE stands for

security envelope or secure encapsulation). If an integrity service is desired, an integrity check value is computed and appended to the PDU. If confidentiality is desired, the entire T-PDU, including a previously appended integrity check value, is enciphered. A receiver, in possession of the correct security attributes (e.g., a cryptographic key), can decipher the SE T-PDU, verify its integrity and then process the resulting T-PDU.

APPENDIX 2. SYSTEM AND NETWORK ARCHITECTURE

2.1 NETWORK MANAGEMENT

MANAGEMENT INFORMATION

For the definitions of management information, this version of the IGOSS (Version 1) focuses primarily on identifying the information required for managing implementations incorporating the functionality specified for layers 1-4 of the OSI Reference Model [ISO 1].

Version 2 of the IGOSS will mainly add the information required for managing implementations of the functions specified for layers 5-7 of the OSI reference model.

SYSTEMS MANAGEMENT FUNCTIONS

The inclusion of the additional Systems Management Functions (SMFs) for Version 2 and subsequent versions of the IGOSS is to be in accordance with the status of the management standards and of the IAs; that is, as the SMFs mature and OIW Implementors Agreements (IAs) are reached on the SMFs, these IAs will be considered for inclusion in the IGOSS. For example, standards are now under development to specify how managing and managed systems are to share management knowledge needed and used in common. These specifications will be referenced in the IGOSS as they become available as international standards.

MANAGEMENT SECURITY

Version 1 of the IGOSS specifies two optional peer-entity authentication modes, Mode 1 (a simple username/password mechanism) and Mode 2 (employs a hash function on the authentication information). Work on Access Control, Confidentiality, Integrity, and Non-repudiation standards is still formative, but these issues will be addressed in future versions of the IGOSS. A goal of the IGOSS is to provide all necessary security services to address the security needs of network management.

NETWORK MANAGEMENT ENSEMBLES

A recently developed concept related to the selection of managed objects (MOs) and system management functions (SMFs) that solves a particular management problem is the concept of "ensembles." Currently, an ensemble is defined as a coherent unit that specifies: 1) the particular problem to be solved, the requirements associated with the problem and a solution to the problem; and 2) the standards and MOs making up the solution. This concept was developed by the Network Management Forum (NMF). The NMF, with cooperation from the OIW, is developing specific ensembles (e.g., the OSI Interworking Ensemble and the Reconfigurable Circuit Service: Configuration Management (RCS) Ensemble). While more work needs to be done, the concept appears to have merit and offers potential for assisting in the preparation of procurement specifications for NM products. As the ensembles concept and the definitions of the ensembles mature and stabilize, consideration will be made on whether or not to include ensembles in future versions of the IGOSS.

2.2 MULTIPEER/MULTICAST (MPMC) COMMUNICATIONS

Broadcast systems have a single communication channel that is shared by all end systems on a subnetwork. MPMC communications allows data to be sent to a subset of these end systems in a single transmission.

REQUIREMENT

The proliferation of large scale distributed systems architectures and the evolution of new applications (e.g. resource location, conferencing, multi-media, management) have highlighted the requirement for the incorporation of MPMC communications in OSI. MPMC communications provide more efficient transmission of data to multiple destinations and communicate with one or more applications whose addresses are unknown or changeable.

STATUS

Recently, ISO and CCITT have begun new projects to address MPMC communications. ISO/IEC JTC1 SC6 has active efforts in defining "Enhanced Communication Functions and Facilities for Lower Layers." These efforts are primarily directed at the development of next generation protocols at the Transport, Network, and Datalink layers. MPMC is a fundamental part of this activity. SC6 also has a distinct activity to incorporate simple connectionless multicast into the suite of existing OSI lower layer protocols. CCITT SGVII is developing multicast network service specifications (X.6) and is working toward the incorporation of MPMC into the OSI architecture.

PLAN

To achieve general support of MPMC in OSI, research, development and standardization are required in the areas of:

- o OSI architecture, to address multi-layer issues and incorporate MPMC communications into the reference model;
- o OSI upper layers, to add facilities to initiate control and exploit MPMC communication; and,
- o OSI lower layers, to add facilities to efficiently provide the underlying multicast service that is fundamental to MPMC communications.

IGOSS organizations will be active technical contributors to the development of the protocols and addressing specifications required to implement the MPMC services.

APPENDIX 3. UPPER LAYERS

3.1 MESSAGE HANDLING SYSTEMS EXTENSIONS

Message Handling Systems (MHS) specifications in Version 1 of the IGOSS are based on the 1984 and 1988 CCITT Recommendations. IGOSS MHS extensions will use the CCITT 1988 MHS Recommendations as a base.

REQUIREMENTS

1. Alignment with functionality in the 1992 Directory Services Recommendations is needed.

2. The CCITT 1988 MHS Recommendations provide a mechanism to define new body parts. New body parts may be needed to meet user requirements.

3. Stable agreements need to be completed for the relatively few X.400 enhancements made in 1992. This included profiling of the Interpersonal Message header extensions and the File Transfer Body Part.

4. Interim MHS Management agreements may be necessary if more rapid progress is not made in this area by CCITT and ISO.

5. Voice Messaging (See CCITT Recommendation X.440) needs to be integrated into MHS.

6. Enhancements to the Message Store service are required, subject to completion of the base standard work in this area.

7. The security requirements of both the U.S. Department of Defense (DoD) and the Canadian Department of Defence (DND) need to be investigated to determine to what extent they can be included in commercial MHS implementations. The U.S. DoD Message Security Protocol should be a starting point in identifying these requirements.

STATUS

Standards - The 1992 CCITT MHS Recommendations are complete and have been formally approved

Implementors Agreements - The intent of the X.400 SIG is to replace the existing Chapter 8 MHS 1988 agreements with a reference to the ISP and only specify additional North American regional requirements. This is made possible because of the high level of technical harmonization that currently exists between the regional agreements.

PLAN

The first six requirements are work items for the MHS SIG. Agreements will be incorporated into the stable workshop document when complete and the services that they provide will appear in MHS products at a later date.

NIST will work with the Defense Information Systems Agency to determine what DoD security services are candidates to be included in commercial implementations. Canada will redraft the COSAC MHS profile to

take into account the additional security services provided by the CCITT 1988 MHS Recommendations in close cooperation with the DND.

3.2 FILE TRANSFER, ACCESS, AND MANAGEMENT (FTAM) EXTENSIONS

The File Transfer, Access and Management Protocol and service allow users on different networks to communicate about files (and transfer files) without requiring that one user know the detailed file characteristics of the other user. A generic file organization is defined for communication; elements of this virtual file model are mapped to corresponding elements of the local file system. A comprehensive set of file attributes and file activity attributes is defined; in addition, a large number of actions is possible on a wide variety of file types.

REQUIREMENTS

Additional requirements for FTAM include the following:

1. filestore management
2. "run length" compression
3. FTAM directory requirements
4. FTAM security
5. use of FTAM to transfer exchange formats
6. advanced adaptive compression

STATUS

Overlapped access and filestore management are nearing IS status as addenda to FTAM.

PLAN

IGOSS organizations will work with the FTAM SIG of the OSE Implementors Workshop to insure that the functionality specified above is incorporated into future implementations.

3.3 REMOTE DATABASE ACCESS EXTENSIONS

Remote Database Access (RDA) allows the interconnection of database applications among heterogeneous environments by providing standard OSI Application layer protocols to establish a remote connection between a database client and a database server. The client is acting on behalf of an application program while the server is interfacing to a process that controls data transfers to and from a database.

REQUIREMENT

The RDA application may be implemented in conjunction with the Basic Application Context or the TP Application Context. The first version of the IGOSS supports only the Basic Application context. The Basic Application Context includes RDA and the ACSE Application Service element and provides a one-phase commit protocol. The TP Application Context provides a two-phase commit which allows updates at multiple remote sites in the same transaction. The TP Application Context includes the following Application Service Elements: RDA, ACSE, TP, and, in provider supported transactions, CCR. Users require the additional services provided by the TP Application Context. Figure A.3.3 shows the application subprofile for RDA TP Application Context implementations.

STATUS

Standards - Remote Database Access Part 1: Generic Model, Service and Protocol (ISO 9579-1) and Remote Database Access Part 2: SQL Specialization (ISO 9579-2) were formally approved as International Standards in 1992.

PLAN

The development of Workshop Agreements for the TP Application Context is expected to commence in 1993.

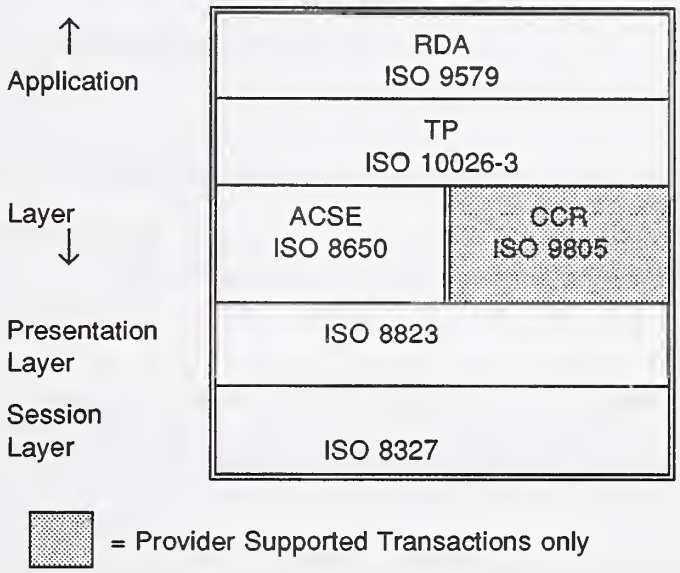


Figure A.3.3. RDA TP Application Context Application Subprofile.

3.4 OSI REMOTE PROCEDURE CALL

The remote procedure call paradigm is the cornerstone of distributed processing systems and client-server architectures. It is used as a building block for advanced services such as distributed file access, remote printing services, and remote execution services. It may also potentially be used across a whole host of applications domains, including office systems, manufacturing, and telecommunications services.

The OSI Remote Procedure Call standard allows application programmers to issue procedure calls to services on remote systems. The OSI Remote Procedure Call standard also specifies a Interface Definition Notation. The notation is used to specify interfaces to remote services. It shields the application programmer from ASN.1.

REQUIREMENTS

Government and industry are beginning to procure distributed processing and remote procedure call systems. The OSI Remote Procedure Call standard allows these systems to interwork with applications on one system accessing services on another. The Interface Definition Notation also promises to provide a common language bridge between an application written in one programming language (e.g., C) and a service written in another (e.g., Ada). As local area networks, proprietary network operating systems, and

proprietary remote procedure call systems are procured, there will be a growing need for OSI Remote Procedure Call to link the systems together. In addition, the OSI Remote Procedure Call standard will allow applications written for one remote procedure call system to be ported to another more easily.

STATUS

The OSI Remote Procedure Call standard (ISO CD 11578) is composed of five parts:

- **Part 1:** Model,
- **Part 2:** Interface Definition Notation,
- **Part 3:** Service,
- **Part 4:** Protocol, and
- **Part 5:** Protocol Implementation Conformance Statement Proforma.

The OSI Remote Procedure Call standard is expected to reach Draft International Standard status in November 1993 and International Standard Status in December 1994.

PLAN

Vendors are likely to begin implementation of the standard in 1993. A Remote Procedure Call SIG should be formed within the OIW. The work items for this new SIG should include:

- Remote Procedure Call API,
- Language Bindings for the Interface Definition Notation (IDN), and
- a Profile for the OSI Remote Procedure Call standard.

The Remote Procedure Call API is necessary for distributed processing tools (e.g., stub compilers) to be used in conjunction with the OSI Remote Procedure Call API. It is important that this API be supportable by proprietary distributed processing systems as well as OSI Remote Procedure Call. The Language Bindings for the Interface Definition Notation will enable interface definitions to be written in standardized programming languages and mapped to the standard Interface Definition Notation. Bindings for C, C++, and COBOL are anticipated. The Profile for the OSI Remote Procedure Call standard will enable implementors' to more quickly and consistently implement the standard.

3.5 DOCUMENT FILING AND RETRIEVAL (DFR)

One of the functions that must be provided in a distributed network is the ability to store and retrieve documents and other files. Document Filing and Retrieval (DFR) specifies the services provided by a file server and the application protocols used between a file server and its clients.

REQUIREMENTS

DFR supports the following features that satisfy user document filing and retrieval requirements:

- o Large capacity document storage for use by multiple users in a distributed system.
- o Order filing and multi-key retrieval.
- o Structure organization of groups of documents.
- o Management of different versions of the same document.
- o Association of attributes with documents and groups.
- o Search by attribute values.
- o Concurrent access to documents and groups.
- o Protection against unauthorized access.
- o Storage of an open-ended number of documents types.

STATUS

ISO 10166 (DFR) is an International Standard in two parts. Part 1 is the Abstract Service Definition and Procedures. Part 2 is the Protocol Specification. DFR is a distributed application located in the Application Layer of the Reference Model for Open Systems Interconnection (see ISO 7498). DFR is also one of a series of International Standards defining applications needed in the area of office automation, as described in the Distributed-office-application-model (ISO 10031-1).

PLAN

In order to produce interoperable DFR products, implementors agreements must be developed by the OSE Implementors' Workshop. It is desirable that these agreements be aligned with DFR profiling work currently underway in other regional workshops.

3.6 DOCUMENT PRINTING APPLICATION

One of the functions that must be provided in a distributed network is the ability to print documents on a printer located remotely from a client workstation or file server. Document Printing Application (DPA) specifies the user and administration services provided by a print server and the application protocols used between a print server and its clients.

REQUIREMENTS

DPA supports the following features that satisfy user document printing requirements:

- o Gives multiple users access to distributed printers.
- o Conveys information concerning scheduling and processing requirements for printing, including special paper or finishing options such as stapling or binding.

- o Provides users with the ability to monitor and manage the progress of print jobs through administrative services.

- o Protects against unauthorized printing of documents.

STATUS

ISO 10175 (DPA) is a Draft International Standard. It is in two parts. Part 1 is the Abstract Service Definition and Procedures. Part 2 is the Protocol Specification. DPA is a distributed application located in the Application Layer of the Reference Model for Open Systems Interconnection (see ISO 7498). DPA is also consistent with the model, architectural framework, and design principles of the Distributed-office-application-model (ISO 10031-2).

PLAN

In order to produce interoperable DPA products, implementors agreements must be developed by the OSE Implementors' Workshop. It is desirable that these agreements be aligned with DPA profiling work that may begin in other regional workshops.

3.7 OSI CLIENT/SERVER MODEL

BACKGROUND

OSI provides application services which operate in a Client/Server environment. A method of designing and procuring services which operate in a Client/Servers environment is needed.

REQUIREMENT

OSI is lacking a distributed computing model for the client/server environment. An OSI Client/Server model is important to users or developers of distributed computing software. The model should include the current and future OSI applications that can operate under this model and the "role" that they play. The model should also include the Application Programming Interfaces that can be used to access Client/Server services.

STATUS

ISO has developed a Distrubuted Office Applications Model (DOAM-ISO 10031) for use in specifying Client/Server services and protocols.

PLAN

The IGOSS organizations will work with the OSE Implementors Workshop to specify an integrated Client/Server profile for distributed computing.

3.8 MINIMAL OSI STACK

Section 3.2.13 in the main body of this document specifies a minimal OSI stack that can be used to provide basic communication services to a wide range of connection oriented network applications that only require the ability to open and close connections and to send and receive messages. Section 3.2.10 specifies how the X-Windows application can be mapped onto the minimal OSI stack.

The Minimal OSI Stack Architecture may be used by other OSI applications that only require basic communications services. These include:

a) FTAM implementations that do not use the recovery service,

b) TP implementations which use only application-supported-transactions, and

c) all ROSE based applications which do not use RTSE

The minimal OSI stack provides all services required by these applications although products which exclusively implement the minimal stack are not yet widely available. The mapping of the OSI applications onto the Minimal OSI stack can be direct or by means of the Applications Programming Interface specified in Appendix 5.

APPENDIX 4. LOWER LAYERS

4.1 Distributed Queue Dual Bus

The Distributed Queue Dual Bus (DQDB) protocol, a protocol used for the Metropolitan Area Network (MAN)/IEEE 802.6, provides for communications at high speed (up to 155 Mbps) over larger distances than was possible with LANs.

The protocol employs a bus architecture and uses a communications reservation system in which each node with data to send notifies its upstream neighbor of its need to transmit. The neighbor then reserves space for the required transmission at the next or a subsequent signaling interval. Thus the transmit queue is said to be distributed.

A dual bus of counter-rotating rings provides both speed and fault tolerance. The direction of data flow on each ring is opposite to the flow of data on the other ring. If a fault occurs in a station or a fiber, the remaining stations can reconfigure the rings to make a single ring including all remaining stations, and data flow continues.

The last station on the bus continually generates empty frames of 125 microseconds each which are broken down into 53 octet segments that are filled by downstream stations.

DQDB fits into the standard IEEE 802 protocol hierarchy. Protocol is specified for the physical layer and Media Access Control (MAC) sublayer of the link layer. The standard IEEE 802.2 specification for Logical Link Control (LLC) fits above the MAC sublayer as it does for the other IEEE 802 LANs.

REQUIREMENT

DQDB is typically used for applications requiring very high speed, high volume data transmission such as CAD/CAM and medical imaging. Since it will soon have an isochronous capability, it will be more widely used, particularly where a high-capacity service is needed to provide enterprise networking including data, voice and full-motion video. There is a requirement to include DQDB as a future IGOSS subnetwork technology.

STATUS

The IEEE 802.6 committee has published the initial version on the DQDB standard. It covers only use with a T3 (44.734 Mbps) facility.

PLAN

The IEEE 802.6 committee is working on a T1 specification, which will be based on the work done by Bellcore in its SMDS specifications. Work is also in progress to permit use of DQDB in SONET and the European digital hierarchy (E1, E3, etc.) Other additions to the standard planned are Isochronous transport, variable bit rate transmission and network management. IGOSS organizations will work with the Lower Layer SIG of the OSE Implementors Workshop to insure that implementation agreements are developed in a timely manner.

4.2 Broadband ISDN (B-ISDN)

Broadband ISDN, an application of cell relay technique using the Asynchronous Transfer Mode standard, is a second generation of ISDN intended eventually to achieve widespread switched service at very high speeds. The key characteristic of B-ISDN is that it provides ISDN services using broadband channels capable of supporting rates greater than the primary ISDN rate. Using SONET as a basis, B-ISDN offers users a virtual circuit service at speeds up to 2 Gbps. Carriers and vendors both may access any portion of the multiplexed signal at any node, adding and dropping any channel in the process. Thus, for example, a node can access a DS1 channel multiplexed into a stream containing both DS1 and DS3 channels, without having to perform multiple levels of demultiplexing, as was necessary with earlier technologies.

B-ISDN is a packet switching technology which achieves its high speed by reducing the error recovery that was a large part of X.25 packet switching service. In addition, it will offer an Isochronous service so that time critical communications, such as voice and full-motion video, can share the facilities with less time-critical data communications.

REQUIREMENT

B-ISDN will be the service of choice for users requiring high speed switched digital service using the public switched network. Internally, carriers who provide the public network will use B-ISDN as the underlying technology for all communications including Plain Old Telephone Service (POTS - the phone company's term for ordinary switched voice communications.) There is a requirement to include Broadband ISDN as a future IGOSS subnetwork technology.

STATUS

Most of the standards underlying B-ISDN have been developed.

PLAN

IGOSS organizations will work with the Lower Layer SIG of the OSE Implementors Workshop to insure that implementation agreements are developed in a timely manner.

APPENDIX 5. APPLICATION PROGRAM INTERFACES

BACKGROUND

In the past, an application was written for a specific hardware/software platform and run at one or two locations. Today, applications are typically run on many different computers, built by different vendors and with different operating systems. It is critical that the increasing investment that is being made in information technology be protected by improving the independence of applications from specific underlying hardware and software platforms. The standardization of selected Application Program Interfaces (APIs) will significantly increase the portability of software by decreasing the need for platform-specific code modules.

REQUIREMENTS

A requirement exists for a portable interface to current and future OSI applications, to common Application Layer services, and to the services provided by the OSI Transport Layer.

At the Application Layer, APIs are currently required for the MHS, FTAM, and Directory Service applications and will soon be required for applications such as Transaction Processing and Remote Database Access when those applications are widely implemented. APIs are also required to provide a portable interface to the common Application Layer services provided by the ACSE and ROSE Application Service Elements.

STATUS

APIs for the Message Handling Systems and Directory Service applications have already been standardized by IEEE committees P1224 and P1003.17 and their use is recommended in Section 3.1.2 of the IGOSS when a portable interface to those OSI applications is required.

An FTAM API is being standardized by the IEEE P1238 working group which will provide a portable interface to high-level FTAM services (e.g., copy a file, delete a file). This API is scheduled to be completed in 1994.

IEEE Committee P1238 is standardizing the XOPEN ACSE/Presentation Service API. This API will permit the developers of OSI and non-OSI applications to use a common upper layer platform for application-level communications and focus development effort on the applications themselves. The XOPEN ACSE/Presentation Service API is already supported by the many vendors.

A ROSE API is being standardized by a new IEEE working group which will provide a portable interface to both high-level and low-level ROSE services. The standard will probably not be completed until the end of 1993.

Transport APIs are being standardized by the IEEE P1003.12 working group which will provide a portable interface to both high-level and low-level Transport services. The high-level interface is referred to as the Simple Network Interface (SNI). The low-level interfaces will be based on Sockets (developed by U.C.-Berkeley) and XTI (developed by X/Open Company Limited). These standards are scheduled to be completed in 1994.

To facilitate access to the Minimal OSI services, a new mapping to mOSI has been developed for XTI by X/Open. The interface is called XTI/mOSI and is specified in Appendix H of the X/Open Transport Interface (XTI). Since XTI provides an interface to a basic connection-oriented service, applications which use XTI

are easily ported to OSI using mOSI with the XTI/mOSI interface. Contact X/Open Company Ltd., 1010 El Camino Road, Suite 380, Menlo Park, CA. 94025 for additional information.

PLAN

IGOSS representatives will work closely with the IEEE to insure that APIs are developed in a timely manner. A recent revision to the charter of the OSI Implementors Workshop (OIW), now the Open Systems Environment (OSE) Implementors Workshop allows this group to also participate in this work. IGOSS representatives will try to insure that the work being done by the IEEE and OIW is coordinated. Additional APIs will be referenced in the next version of the IGOSS; however, the use of standard APIs which meet Federal and commercial needs should be encouraged as soon as they are available from a significant number of vendors.

APPENDIX 6. DIRECTORY SERVICES CONFORMANCE SPECIFICATIONS

6.1 Directory User Agent Conformance Specifications

6.1.1 Supported Types and Levels of Authentication

The following "Authentication Modes" are used in IGOSS procurement categories to specify required combinations of authentication type, level, and direction for a DUA.

Authentication Mode 0

Authentication Mode 0 is supported by a DUA capable of transmitting **DirectoryBindArgument** without **credentials** or with **simplecredentials** containing either:

- o only the name component; or
- o the name component and an unprotected password.

A DUA supporting this Authentication Mode is capable of enabling a DSA, via the DAP, to perform operations when there is no authentication requirement. It should be noted that authentication based on unprotected passwords is not sufficient to satisfy a requirement, expressed in Basic Access Control or Simplified Access Control, for simple authentication. Mode 0 authentication is adequate only when the authentication level requirement in an access control list is specified as "none."

Authentication Mode 1

Authentication Mode 1 is supported by a DUA capable of transmitting **DirectoryBind ARGUMENT** with **SimpleCredentials** containing a protected password.

A DUA supporting this Authentication Mode is capable of enabling a DSA, contacted via the DAP, to perform simple authentication of the user based on a protected password.

Authentication Mode 2

Authentication Mode 2 is supported by a DUA capable of transmitting **DirectoryBind ARGUMENT** containing **StrongCredentials.** A DUA supporting this Authentication Mode is capable of enabling a DSA, contacted via the DAP, to perform strong authentication of the user at the time when the DAP connection is established.

Authentication Mode 3

Authentication Mode 3 is supported by a DUA capable of producing and transmitting the digitally-signed variant of abstract operation arguments. The DUA shall use the private key of the user to generate the digital signature, and shall include the name, time, and random components of **SecurityParameters** within **CommonArguments.**

A DUA supporting this Authentication Mode is capable of enabling a DSA, contacted via the DAP or DSP, to perform strong authentication of the user each time an abstract operation, with signed arguments, is submitted to that DSA. This Authentication Mode enables any DSA involved in responding to a chained or decomposed operation request to directly perform strong authentication of the user.

Authentication Mode 4

Authentication Mode 4 is supported by a DUA capable of receiving a signed result (an abstract operation result and **DirectoryBind RESULT**) and validating the signature. A DUA supporting this Authentication Mode is capable of performing strong authentication of the DSA that signed the result.

6.1.2 Miscellaneous Conformance Requirements for IGOSS DUAs

All conformant DUA products shall satisfy the following requirements.

1. An IGOSS conformant DUA shall, as a minimum, support Authentication Modes 0 and 1.

2. An IGOSS conformant DUA shall support character set requirements specified in Part 11, clause 7.1 of the Workshop Agreements.

3. An IGOSS conformant DUA shall perform normalization of protocol elements containing Universal Coordinated Time according to the rule specified in Part 11, clause A.4.1 of the Workshop Agreements.

4. Certain 1993 extensions to the abstract operations must also be supported as follows:

a) "Administrative" DUAs shall support the **extraAttributes** extensions.

b) "Administrative" DUAs shall support the **subentries** extension.

c) "Administrative" DUAs shall support the **newSuperior** extension.

d) "Adminstrative" DUAs shall support the **useAliasOnUpdate** extension.

6.2 Directory Service Agent Conformance Specifications

6.2.1 DSA: Supported Types and Levels of Authentication

DSA Authentication Modes associated with DUA - DSA interaction are compatible with those defined previously in this Appendix. For example, a DUA supporting Authentication Modes 0 and 1 can be used with a DSA that supports Authentication Modes 0 and 1. Also, a DUA supporting Mode 2 can be used with a DSA that supports Mode 2; a DUA supporting Mode 3 can be used with a DSA that supports Mode 3. A DUA that supports Authentication Mode 4 can be used with a DSA that supports Mode 4 and/or Mode 5.

This Appendix also defines the modes associated with DSA - DSA interaction that are used to perform peer-entity authentication between DSAs cooperating in a chained operation. These modes are primarily used to allow a responding DSA to determine whether each DSA in a chain is (via bilateral agreement) trusted to properly handle chaining arguments, apply peer-entity authentication, and enforce access controls. The measure of trustworthiness of a chain depends on: (1) the trustworthiness of the **TraceInformation;** (2) whether each DSA listed in **TraceInformation** is known to be trusted; and (3) what mode of peer-entity authentication was performed by each DSA in the chain. The decision to procure a particular authentication mode from among modes 4, 6, and 7 should be based on a security policy establishing the level of confidence required before a chain is considered trustworthy. A trust domain in which each DSA uses mode 7 generally provides a relatively low level of confidence because it is based on protected passwords and there is no integrity check on **TraceInformation.** A trust domain in which

each DSA uses mode 4 generally provides a medium level of confidence because even though strong authentication is being performed at bind time, there is no integrity check on **TraceInformation.** Mode 6 generally provides the highest level of confidence because it uses strong authentication in the form of signed operation arguments to provide an integrity check on each instance of **TraceInformation**.

The following Authentication Modes are used in IGOSS procurement categories to specify required combinations of authentication type, level, and direction for a DSA.

Authentication Mode 0

Authentication Mode 0 is supported by a DSA capable of performing user authentication, based on the **DirectoryBind ARGUMENT,** using **SimpleCredentials** containing either: the name component only; or the name component and an unprotected password.

For the purpose of enforcing access control (Basic Access Control or Simplified Access Control), the DSA shall associate this mode with **AuthenticationLevel "none"** (see definition of **AuthenticationLevel** clause 15 of [CCITT 38]). In other words, for the purpose of enforcing access control, this mode is considered to provide no justification for believing that the purported user is, in fact, the actual user. This mode is the weakest form of user authentication and is highly vulnerable to masquerading and replay attacks.

Conformance to this mode also requires that when a DSA (supporting the DSP initiator role) initiates a chained operation and has successfully authenticated the user under mode 0, that DSA shall set the **AuthenticationLevel** element of **ChainingArguments** to **"none."**

Authentication Mode 1

Authentication Mode 1 is supported by a DSA capable of performing user authentication, based on **DirectoryBind ARGUMENT,** using **SimpleCredentials** containing a protected password.

For the purpose of enforcing access control (Basic Access Control or Simplified Access Control), the DSA shall associate this mode with **AuthenticationLevel "simple"** (see definition of **AuthenticationLevel** in clause 15 of [CCITT 38]).

Conformance to this mode also requires that when a DSA (supporting the DSP initiator role) initiates a chained operation and has successfully authenticated the user under mode 1, the DSA shall set the **AuthenticationLevel** element of **ChainingArguments** to **"simple."** If the initiating DSA does not authenticate the user under mode 1 before chaining the operation, the DSA shall omit **AuthenticationLevel** within **ChainingArguments.**

Authentication Mode 2

Authentication Mode 2 is supported by a DSA capable of performing strong authentication of the user at the time when a DAP connection is established. The authentication is based on **StrongCredentials** received in the **DirectoryBind ARGUMENT.**

For the purpose of enforcing access control (Basic Access Control or Simplified Access Control), a DSA shall associate this mode with **AuthenticationLevel "strong"** (see definition of **AuthenticationLevel** in clause 15 of [CCITT 38]).

Conformance to this mode also requires that when a DSA (supporting the DSP initiator role) initiates a chained operation and has successfully authenticated the user under mode 2, the DSA shall set the **AuthenticationLevel** element of **ChainingArguments** to **"strong."**

Authentication Mode 3

Authentication Mode 3 is supported by a DSA capable of performing strong authentication of the user by verifying the digital signature on the abstract operation arguments and checking for replay attack.

For the purpose of enforcing access control (Basic Access Control or Simplified Access Control), a DSA shall associate this mode with **AuthenticationLevel** "strong" (see definition of **AuthenticationLevel** in clause 15 of [CCITT 38]).

Conformance to this mode also requires that when a DSA (supporting the DSP initiator role) initiates a chained operation and has successfully authenticated the user under mode 3, the DSA shall set the **AuthenticationLevel** element of **ChainingArguments** to **"strong."**

Authentication Mode 4

Authentication Mode 4 is supported by a DSA capable of performing two-way peer-entity strong authentication at bind time when a DAP, DSP, DISP or DOP association is established.

Authentication Mode 4 is supported by a DSA capable of:

1. validating a DSA's signature, including detection of replay attack, as received in **StrongCredentials** of a bind argument;

2. digitally signing the **Token** in **StrongCredentials** transmitted in a bind result;

3. digitally signing the **Token** in **StrongCredentials** transmitted in a bind argument.

Authentication Mode 5

Authentication Mode 5 is supported by a DSA capable of producing and transmitting the digitally signed varient of abstract operation results. This capability enables origin authentication and integrity checking of the results. The signing DSA shall include the name, time, and random components of **SecurityParameters** within **CommonArguments**.

Authentication Mode 6

Authentication Mode 6 is supported by a DSA capable of performing all of the functions defined in mode 5 and, in addition, is capable of: (1) verifying a DSA's digital signature on abstract operation arguments; and (2) applying its own signature to abstract operation arguments in preparation for chaining the operation to another DSA. The signing DSA shall include the name, time, and random components of **SecurityParameters** within **CommonArguments**. Verification of signature includes checking for replay attack.

Authentication Mode 7

Authentication Mode 7 is supported by a DSA capable of performing two-way peer-entity simple protected authentication at bind time when a DSP, DISP, or DOP association is established.

Authentication Mode 7 is supported by a DSA capable of:

1. validating a DSA's protected password, as received in **SimpleCredentials** of a bind argument;
2. transmitting its protected password in **SimpleCredentials** of a bind result; and
3. transmitting its protected password in **SimpleCredentials** of a bind argument.

6.2.2 DSA: Supported Attributes and Object Classes

An IGOSS conformant DSA shall support all Selected Attribute Types defined in clause 5 of [ISO 75]. A conformant DSA shall support all attribute syntaxes defined in clause 6 of [ISO 75]. A conformant DSA shall support all matching rules defined in clause 7 of [CCITT 43].

A conformant DSA that supports any form of strong authentication shall support the following attribute types described in [CCITT 39]: **UserCertificate, CACertificate, CrossCertificatePair, CertificateRevocationList, and AuthorityRevocationList.** A conformant DSA shall support **UserPassword** described in [CCITT 39].

In addition, a conformant DSA shall be configurable to allow new attribute types to be defined by the DSA administrator. Extensibility of supported attribute types shall include the following features:

- o new types may be defined in terms of syntax described in clause 6 of [CCITT 43];
- o new types may be defined in terms of new syntax where:

  1. the syntax is one of the following: Integer, Null, Boolean, Enumerated, Bit String, Octet String, object identifier, Distinguished Name, Case Exact String, Case Ignore String, Numeric String, Printable String, UTC Time, and Telephone Number;

  2. the new syntax is an ASN.1 structured type (i.e., SET, SEQUENCE, SET OF, SEQUENCE OF, and CHOICE), possibly including tags, where each component uses one of the syntax forms listed in the previous item;

  3. the matching rule associated with a locally defined type may be defined using any of the rules described in clause 7 of [CCITT 43].

An IGOSS conformant DSA shall support all Selected Object Classes defined in clauses 6.1 through 6.13 of [CCITT 44]. A DSA which supports any form of strong authentication shall support **strongAuthenticationUser** and **certificationAuthority** as defined in clauses 6.14 and 6.15 of [CCITT 44].

An IGOSS conformant DSA shall be configurable to allow new object classes or subclasses to be defined by the DSA administrator. Extensibility of supported object classes shall include the following features:

- o new object classes may be defined to be either abstract, structural, or auxiliary;
- o a new object class may be a subclass of any class described in [CCITT 44] or it may be a subclass of a locally defined class.
- o a new object class may be defined in terms of any combination of attribute types described in [CCITT 43] and locally defined attribute types.

6.2.3 DSA: Support For Name Bindings

An IGOSS conformant DSA shall be configurable to allow the DSA administrator to define the complete set of allowed name bindings. Each of the name bindings described in clause 7 of [CCITT 43] shall be implemented.

6.2.4 DSA: Support For Hierarchical Attributes

Hierarchical attributes work in conjunction with the **extendedFilter** feature to provide a mechanism for grouping attributes such that the group has a generic type that can be used to retrieve the entire group. For example, the generic type "telephoneNumber" could be defined to include subtypes such as work phone number, organizational phone number, and fax number. The generic type can be used in a filter to return any of the subtypes. The support of hierarchical attributes is mandatory. Hierarchical attribute types are described in clause 11.4 of [CCITT 38].

6.2.5 DSA: Support For Collective Attributes

Collective attributes provide a convenient way to specify an attribute which is common to many entries. For example, all the employees of a given organization might have the same fax number. Using collective attributes, the attribute can be entered into a single subentry whose scope includes all the entries to which it applies; this might be more efficient than entering the fax number into each employee's entry. Support for collective attributes is mandatory. Collective attributes are described in clause 11.4 of [CCITT 38].

6.2.6 DSA: Support For Operational Attributes

All IGOSS conformant DSAs shall support operational attributes associated with the supported access control scheme(s). All IGOSS conformant DSAs shall support **createTimestamp, modifyTimestamp, creatorsName,** and **modifiersName.**

6.2.7 DSA: Capability To Support Root Naming Context

All IGOSS conformant DSAs shall be capable of supporting the root context, as specified for first-level DSAs in [CCITT 41].

6.2.8 DSA: Support For Access Control

The 1993 edition of the Directory standard provides two access control mechanisms: Simplified Access Control (SAC) and Basic Access Control (BAC). An IGOSS conformant DSA shall support Simplified Access Control. Support for Basic Access Control is optional. A class 2 subtree specification, as defined in Part 11, clause 8.10 of the Workshop Agreements shall be supported. When BAC is implemented, the DSA shall provide a means whereby a superior authority can positively control the maximum precedence that may be assigned within an **ACIItem** by a subordinate authority.

The DSA shall determine if a chain is trustworthy before using it to return any abstract operation result or error result that contains information subject to access control. The DSA shall determine if the chain is trustworthy before believing the **AuthenticationLevel** received in **ChainingArguments**; when the chain is found to be untrustworthy, the DSA shall, for the purpose of making access control decisions, assign the level of "none" to the requesting user. When **ChainingArguments** do not include **AuthenticationLevel** the DSA shall assign the level of "none" to the requesting user.

When the DSA supports only one of the modes 4, 5, or 7, it shall use that mode when determining if the chain is trustworthy. When the DSA is configurable in this regard, it shall use the mode (4, 5, or 7) designated by the system administrator when determining if the chain is trustworthy.

6.2.9 Miscellaneous Conformance Requirements For All IGOSS DSAs

The following miscellaneous requirements shall be satisfied by all IGOSS DSAs:

1. Adhere to the pragmatic constraints specified in Part 11, clause 7 of the Workshop Agreements;

2. Adhere to the requirements in Part 11, Annex A of the Workshop Agreements regarding Maintenance of Attribute Syntaxes;

3. Adhere to the requirement to support Session Version 2 as described in Part 11, clause 10.2 of the Workshop Agreements.

6.2.10 Miscellaneous Conformance Requirements For IGOSS Cooperative DSAs

The following miscellaneous requirements shall be satisfied by all IGOSS cooperative DSAs:

1. Be able to carry out name resolution and search continuation for an alias whose dereference points to an entry held outside the DSA as described in Part 11, clause 9.1.5 of the Workshop Agreements.

2. Be able to carry out simple authentication of a user whose entry is outside the authenticating DSA as described in Part 11, clause 9.1.7 of the Workshop Agreements.

3. Adhere to requirements regarding the handling of **TraceInformation** specified in Part 11, clause 9.2.2 of the Workshop Agreements.

4. Adhere to the requirement regarding propagation of signed arguments specified in Part 11, clause 9.2.3 of the Workshop Agreements.

5. Adhere to the requirements regarding referrals and chaining specified in Part 11, clause 9.2.4 of the Workshop Agreements with the following proviso:

The first paragraph of Part 11, clause 9.2.4 of the Workshop Agreements states conditions under which a chaining DSA does not act on a referral. For the purpose of this specification, the conditions include the following:

- o the **returnToDUA** element of **DSAReferral** indicates the referral is not to be acted on; or
- o administrative limitations or service policies prevent the DSA from acting on the referral;

6. Adhere to underlying services requirements specified in Part 11, clause 10 of the Workshop Agreements.

7. Implement the Directory Information Shadowing Protocol as described in Part 11, clause 8.11 of the Workshop Agreements. A class 2 unit of replication, as described in Part 11, clause 8.11.3 of the Workshop Agreements, shall be supported.

6.2.11 Miscellaneous Conformance Requirements for IGOSS Solitary DSAs.

A Solitary DSA product shall not implement shadowing.

APPENDIX 7. ACRONYMS

ACE	Association Control Service Element
ADMD	Administration Domain
AE	Application Entity
AFI	Authority Format Identifier
ANSI	American National Standards Institute
API	Application Programming Interface
ARM	Alarm Reporting Function
ARR	Attributes for Representing Relationships
ASE	Application Service Element
ASN	Abstract Syntax Notation
B-ISDN	Broadband ISDN
BAC	Basic Access Control
BRI	Basic Rate Interface
CAD	Computer Aided Design
CAM	Computer Aided Manufacturing
CC	Connect Confirm
CCITT	Consultative Committee for International Telegraphy and Telephony
CCR	Commitment, Concurrency and Recovery
CCTA	Central Computer and Telecommunications Agency
CD	Committee Draft
CFM	Configuration Management
CGM	Computer Graphics Metafile
CLNS	Connectionless Network Service
CLTS	Connectionless Transport Service
CLUL	Connectionless Upper Layer
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CONS	Connection Oriented Network Service
COS	Corporation for Open Systems
COSAC	Canadian Open Systems Application Criteria
COTS	Connection Oriented Transport Service
CR	Connect Request
CSA	Canadian Standards Association
CSMA/CD	Carrier Sense, Multiple Access with Collision Detection
CTS3/NM	European Community Testing Service for Network Management
DAM	Draft Amendment
DAP	Directory Access Protocol
DCE	Data Circuit-terminating Equipment
DES	Data Encryption Standard
DFI	DSP Format Identifier
DFR	Document Filing and Retrieval
DIS	Draft International Standard
DISP	Directory Information Shadowing protocol
DIT	Directory Information Tree
DMI	Definitions of Management Information
DOP	Directory Operational Binding Management Protocol
DPA	Document Printing Application
DQDB	Distributed Queue Dual Bus

DR	Disconnect Request
DSA	Directory Service Agent
DSP	Directory System Protocol
DSP	Domain Specific Part
DTE	Data Terminal Equipment
DUA	Directory User Agent
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EIA	Electronic Industries Association
EPRI	Electric Power Research Institute
ERMF	Event Report Management Function
ES	End System
ES-IS	End System-Intermediate System
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FTAM	File Transfer, Access, and Management
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
HDLC	High Level Data Link Control
HMI	Human Machine Interface
IA	Implementation Agreement
ICD	International Code Designator
IDI	Initial Domain Identifier
IDP	Initial Domain Part
IDRP	Inter-Domain Routing Protocol
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IGES	Initial Graphic Exchange Specification
IGOSS	Industry/Government Open Systems Specification
IIW	ISDN Implementors Workshop
INTAP	Interoperability Technology Association for Information Processing
IPM	Interpersonal Messing
IR	Information Retrieval
IS	Intermediate System
IS	International Standard
IS-IS	Intermediate System-Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	International Standardized Profile
IT	Information Technology
JTC	Joint Technical Committee
LAN	Local Area Network
LAPB	Link Access Procedure B
LAPD	Link Access Procedure D
LCF	Low Cost Fiber
LCF	Log Control Function
LLC	Logical Link Control
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Manufacturing Automation Protocol
MHS	Message Handling Systems
MIB	Management Information Base

MIT	Massachusetts Institute of Technology
MMF	Multimode Fiber
MMS	Manufacturing Messaging Specification
MO	Managed Object
mOSI	Minimal OSI
MPMC	Multipeer/Multicast
MS	Message Store
MTA	Message Transfer Agent
MTS	Message Transfer System
NBS	National Bureau of Standards
NCS	National Communications System
NIST	National Institute of Standards and Technology
NIUF	North American ISDN Users Forum
NLSP	Network Layer Security Protocol
NM	Network Mangement
NMF	Network Mangement Forum
NPAI	Network Protocol Address Information
NSAP	Network Service Access Point
O/R	Originator/Recipient
ODA	Office Document Architecture
OIW	OSE Implementors Workshop
OMF	Object Management Function
OMG	Object Management Group
OMNI	Open Management Interoperability
OSE	Opens Systems Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
PAD	Packet Assembler/Disassembler
PCM	Physical Connection Management
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PLP	Packet Level Protocol
PMD	Physical Media Dependent
PMF	Parameter Management Frames
PPP	Point to Point Protocol
PRI	Primary Rate Interface
PRMD	Private Management Domain
POTS	Plain Old Telephone Service
PVC	Permanent Virtual Circuit
RDA	Remote Database Access
RDN	Relative Distinguished Name
RFC	Request for Comments
RMT	Ring Management
ROSE	Remote Operation Service Element
RTSE	Reliable Transfer Service Element
SAC	Simplified Access Control
SARF	Security Alarm Reporting Function
SDNS	Secure Data Network System
SE	Security Envelope
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIG	Special Interest Group

SMF	Systems Management Function
SMF	Single Mode Fiber
SMT	Station Management
SNARE	Subnetwork Address Resolution Entities
SNI	Single Network Interface
SONET	Synchronous Optical Network
SPAG	Standards Promotion and Application Group
SQL	Structured Query Language
SSL	Standard Security Label
STEP	Standard for the Exchange of Product Model Data
STMF	State Management Function
SVC	Switched Virtual Circuit
TBITS	Treasury Board Information Technology Standard
TLSP	Transport Layer Security Protocol
TOP	Technical and Office Protocols
TP	Transaction Processing
TPDU	Transport Protocol Data Unit
TPSU	Transaction Processing Service Unit
U-ASE	User Application Service Element
UA	User Agent
UAC	User Advisory Council
UCA	Utility Communication Architecture
UI	Unix International
VT	Virtual Terminal
WAN	Wide Area Network
WG	Working Group
XTI	X-Open Transport Layer Interface

☆ U.S. GOVERNMENT PRINTING OFFICE: 1994 — 300-568/04033

ANNOUNCEMENT OF NEW PUBLICATIONS ON COMPUTER SYSTEMS TECHNOLOGY

Superintendent of Documents
Government Printing Office
Washington, DC 20402

Dear Sir:

Please add my name to the announcement list of new publications to be issued in the series: National Institute of Standards and Technology Special Publication 500-.

Name _____

Company _____

Address _____

City _____ State _____ Zip Code _____

(Notification key N-503)

NIST Technical Publications

Periodical

Journal of Research of the National Institute of Standards and Technology—Reports NIST research and development in those disciplines of the physical and engineering sciences in which the Institute is active. These include physics, chemistry, engineering, mathematics, and computer sciences. Papers cover a broad range of subjects, with major emphasis on measurement methodology and the basic technology underlying standardization. Also included from time to time are survey articles on topics closely related to the Institute's technical and scientific programs. Issued six times a year.

Nonperiodicals

Monographs—Major contributions to the technical literature on various subjects related to the Institute's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of conferences sponsored by NIST, NIST annual reports, and other special publications appropriate to this grouping such as wall charts, pocket cards, and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a worldwide program coordinated by NIST under the authority of the National Standard Data Act (Public Law 90-396). NOTE: The Journal of Physical and Chemical Reference Data (JPCRD) is published bimonthly for NIST by the American Chemical Society (ACS) and the American Institute of Physics (AIP). Subscriptions, reprints, and supplements are available from ACS, 1155 Sixteenth St., NW, Washington, DC 20056.

Building Science Series—Disseminates technical information developed at the Institute on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NIST under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The standards establish nationally recognized requirements for products, and provide all concerned interests with a basis for common understanding of the characteristics of the products. NIST administers this program in support of the efforts of private-sector standardizing organizations.

Consumer Information Series—Practical information, based on NIST research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

Order the **above** *NIST publications from: Superintendent of Documents, Government Printing Office, Washington, DC 20402.*

Order the **following** *NIST publications—FIPS and NISTIRs—from the National Technical Information Service, Springfield, VA 22161.*

Federal Information Processing Standards Publications (FIPS PUB)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The Register serves as the official source of information in the Federal Government regarding standards issued by NIST pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations).

NIST Interagency Reports (NISTIR)—A special series of interim or final reports on work performed by NIST for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service, Springfield, VA 22161, in paper copy or microfiche form.

U.S. Department of Commerce
National Institute of Standards and Technology
Gaithersburg, MD 20899